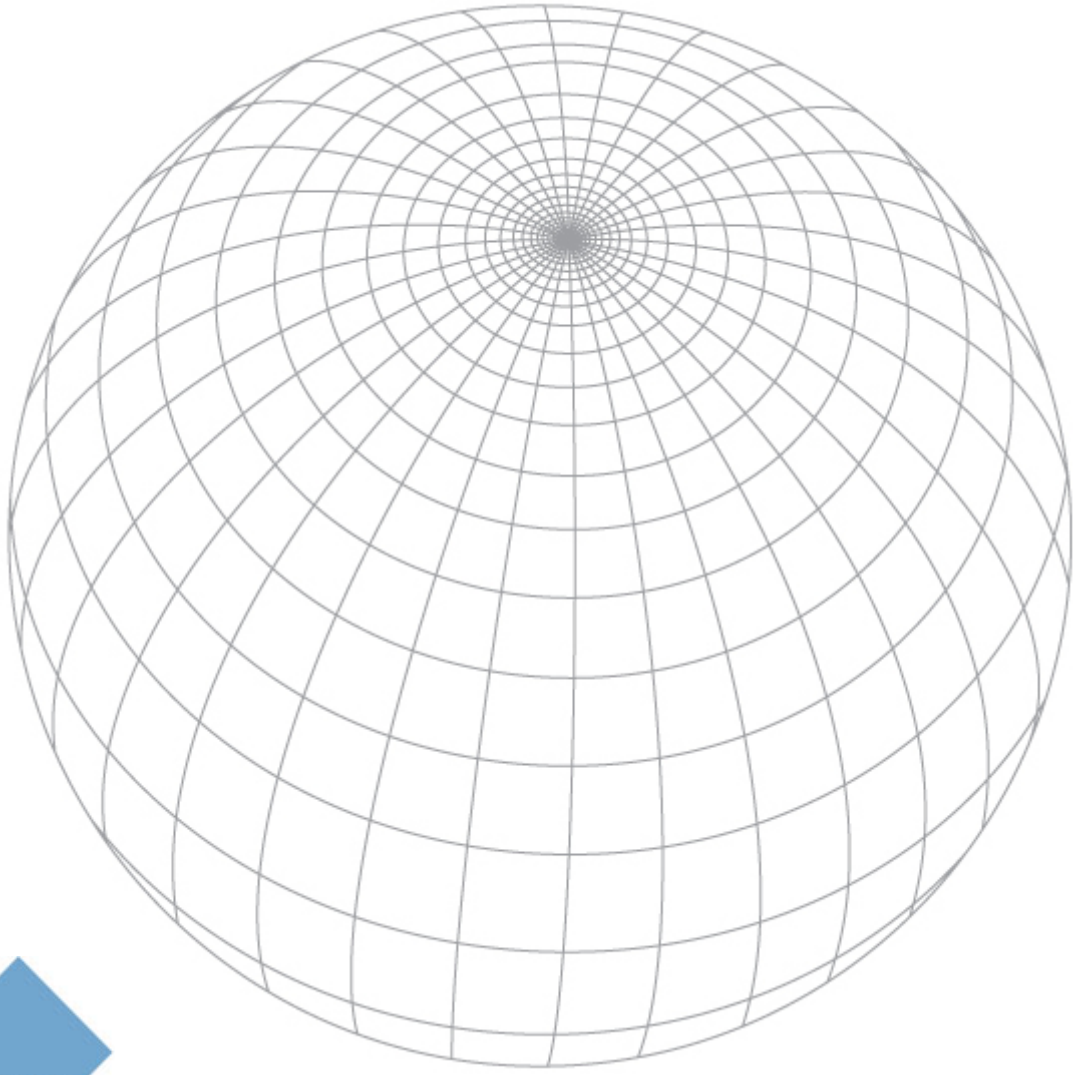
milestone

XProtect

Enterprise 6.5

Administrator's Manual



milestone

Target Audience for this Document

This document covers Milestone XProtect Enterprise from a surveillance system administrator's perspective. It is solely aimed at XProtect Enterprise system administrators, and administrator rights are likely to be required in order to be able to access the majority of features described in this document.

This document provides detailed descriptions of XProtect Enterprise system administration features. It furthermore provides a large number of targeted "how-to" examples, guiding administrators through completing common administration tasks in XProtect Enterprise.

This document contains very limited end-user related documentation. Administrators requiring information about end-user related applications, such as the remote access clients, should refer to the targeted manuals available on the XProtect Enterprise software DVD as well as from www.milestonesys.com.

Users who do not have surveillance system administrator responsibilities—such as users of the Viewer, Remote Client, Smart Client, PDA Client, or Matrix Monitor—will find that this manual is not of relevance to them. Such users will be able to find information targeted at their needs in the separate manuals available on the XProtect Enterprise software DVD as well as from www.milestonesys.com.

Copyright, Trademarks and Important Information

Copyright

© 2009 Milestone Systems A/S.

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This document is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserve the right to make adjustments without prior notification.

All names of people and organizations used in this document's examples are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

Contents

INTRODUCTION 14
Product Overview 14
Several Targeted Components in One 14
Updates 15

REQUIREMENTS AND PREREQUISITES 16
System Requirements 16
Surveillance System Server 16
Smart Client 16
Remote Client 17
PDA Server 17
PDA Client 18
Matrix Monitor 18
Important Port Numbers 19
Time Server Recommended 20

ADMINISTRATORS' GETTING STARTED CHECKLIST 21

INSTALLATION 24
Microsoft® Windows® Vista® Information 24
Installing the Server Software 24
Upgrading from a Previous Version 25

USING THE BUILT-IN HELP SYSTEM 28

THE ADMINISTRATOR APPLICATION 30
Administrator Login Window 30
Administrator Window 30

Device Manager Section 30
Adding Devices 31
Editing Settings for Devices 31
Editing Settings for Cameras 31
Renaming Cameras 31
Assigning Shortcut Numbers to Cameras 31
Editing Settings for Audio Sources 31
Disabling/Enabling Cameras and Audio Sources 31
Administrator Window's Buttons 32

DEVICE LICENSE KEYS (DLKS) 35
How to Import Device License Keys 35

IP DEVICE ADMINISTRATION 36
How to Add a Device 36
Edit Device Settings Window 38
Camera Settings for [Device Name] Window 40
Using DVR Devices 42

CAMERA ADMINISTRATION 43
Adding and Configuring Cameras 43
Camera Settings for [Device Name] [Camera Name] Window 43
Speedup Settings 44
Recording Settings 44
Live Settings 45
Audio 45
Fisheye 46
Motion Detection Settings 46
Database Settings 46
Database Resizing 48
Image Quality 49
Event Notification 49
Outputs 49
PTZ Present Position (PTZ Cameras Only) 49

Configure Device Window 50
Camera Settings Section 50
Preview Image 50
Adjust Motion Detection Window 50
Noise Sensitivity 51
Motion Sensitivity 51
Define Exclusion Regions Window 52
Defining Areas in which Motion Detection Should Be Disabled 52
Output Settings for [Device Name] [Camera Name] Window 53
Associating Outputs with Manual Control and Detected Motion 53
Setup Notifications on Events Window 54
What is an Event Indication? 55
Specifying Events for which Event Indication Should Be Used 55
PTZ Preset Positions for [Device Name] [Camera Name] Window 56
Why Use Preset Positions? 56
Absolute and Relative Positioning PTZ Cameras 56
How to Define a Preset Position 56
Event Window (for PTZ Preset Positions on Events) 59
Associating Preset Positions with Particular Events 59
Setup PTZ Patrolling Window 60
Patrol Scheme 60
Selecting Preset Positions to Be Used for a PTZ Patrol Scheme 61
Specifying Timing Settings for a PTZ Patrol Scheme 61
PTZ Patrolling Actions on Detected Motion 62
PTZ Scanning 62
Fisheye Camera Configuration Window 62
Fisheye View Adjustment 63
Previewing the Fisheye View 63
Ceiling Mounted Cameras 64
Setting a View as Home Position 64
Image Resolution 64
Camera Name and Number Window 64

AUDIO SOURCE ADMINISTRATION 66
Important Information about Using Audio 66
Microphone Settings Window 67

Speaker Settings Window 67

RECORDING SERVER SERVICE MANAGEMENT 68

Using the Recording Server Manager 68

Starting and Stopping the Recording Server 68

Opening the Administrator Application 68

Monitoring System Status 68

Viewing Recording Server & Image Server Log Files 69

Service Manager Window 70

Pausing the Milestone Recording Server Service 70

Resuming the Milestone Recording Server Service 70

What to Do if the Milestone Recording Server Service is Stopped 70

SCHEDULING 71

Camera/Alert Scheduler Window 71

How to Set or Clear Periods in the Calendar 73

Colored Bars 74

How to Copy and Paste Schedules 74

GENERAL SETTINGS 76

General Settings Window 76

Administrator Settings 76

Changing the Administrator Password 76

Manual Start Recording Settings 76

Milestone XProtect Central Settings 76

Patrolling Settings 77

Logfile Settings 77

Event Recording Settings 77

Advanced 78

Email Settings 79

Sms Settings 79

Change Password Window 79

How to Change the Administrator Password 79

Milestone XProtect Central Settings Window 79

E-Mail Setup Window 80
Enabling E-mail Alerts 80
Specifying Recipients 81
Specifying Sender Settings 81
Specifying Default Subject and Message Texts 81
Specifying Image and Interval Options 81
Testing Your E-Mail Alert Configuration 82
SMS Settings Window 82
Enabling SMS Alerts 82
Specifying SMS Alert Settings 82
Testing Your SMS Alert Configuration 83

INPUT, EVENTS & OUTPUT 84
About Input, Events & Output 84
Types of Events 84
Specifying Input, Events and Output 85
Using Dedicated I/O Devices 85
I/O Setup 86
I/O Setup Window 86
Using the I/O Setup Window's Defined Events List and Buttons 86
Add New Event Window (for Devices Capable of Handling One Input Only) 88
Multiple Input Events Window 90
Add New Event Window (for Devices Capable of Handling Several Inputs) . 91
Edit Event Window (for Editing Input Events) 92
New Timer Window 93
Add New Output Window 94
Testing the Defined Output 94
Edit Output Window 94
Testing the Defined Output 95
Advanced Window 95
Port Numbers and Polling Frequency 95
Event Buttons 96
What Is an Event Button? 96
Event Buttons Window 96
Defined Events List 97
Specifying Event Buttons and Timer Events 97

Specifying Global Event Buttons 97
Specifying Camera-Specific Event Buttons 97
Specifying Timer Events 97
Editing Event Buttons and Timer Events 98
Associating Event Buttons with External Outputs 98
Add New Event Window (for Adding Event Buttons) 98
Edit Event Window (for Editing Event Buttons) 99
Generic Events 100
Generic Events Window 100
Add New Event Window (for Specifying Generic Events) 101
General Event Settings Section 101
Event Rule String Section 102
Notification Settings Section 104
Edit Event Window (for Editing Generic Events) 104
Input/Output Control 105
I/O Control Window 105
Associating Event with Particular Outputs 105
Output Settings for [Device Name] [Camera Name] Window 106
Associating Outputs with Manual Control and Detected Motion 106
Selecting Output for Manual Control 106
Selecting Output for Use on Motion Detection 106
How to 107
How to Add an Input-Based Event 107
How to Add an Event Button 108
How to Add a VMD Event 110
How to Add a Generic Event 112
How to Test a Generic Event 114
How to Add a Timer Event 116
How to Add a Manually Controlled Output 118
How to Add a Motion-Triggered Output 121

ARCHIVING 125
Benefits of Archiving 125
How Archiving Works 125
Storing Archives at Other Locations than the Default Archiving Directory .126
Archiving Audio 126

Storage Capacity Required for Archiving....126
Automatic Response if Running Out of Disk Space....127
Backing Up Archives....128
Viewing Archived Recordings....129
Virus Scanning and Archiving....129
New Database if Archiving Fails....129
Archive Setup Window....130
Static Archiving....133
Dynamic Archiving....134
Archiving Audio....134

MATRIX ADMINISTRATION....135
Matrix Configuration Window....135
Enabling Matrix and Defining Matrix Recipients....135
Automatic Matrix Display on Events....137

IMAGE SERVER ADMINISTRATION....139
Image Server Administrator Window....139
Server Configuration Section....139
User Administration Section....141
Defining Users....141
Defining User Access Rights....141
Full Access for All Users....141
Restricted Access....141
Master/Slave Setup Section....141
Configuration on the Master Server....142
Configuration on a Slave Server....142
If Not Using a Master/Slave Setup....142
Upgrading Servers in an Existing Master/Slave Setup....142
Log Files Section....143
Audit Log Section....143
Language Support and XML Encoding Section....143
Good to Know: Client Access to Stopped Cameras....144
Define Local IP Ranges Window....144
User Administration Window....144

What Is Active Directory?....145
How to Add a New Basic User....146
How to Add a New Windows User or Group....146
How to Edit an Existing User Name or Password....147
How to Remove an Existing User....147
What Information to Provide to Users....147
Define User Rights Window....148
Slave Administration Window....151
Adding a Slave Server....151
Removing a Slave Server....151
End-User Documentation....151

DOWNLOAD MANAGER....152
The Welcome Page....152
Download Manager's Default Configuration....153
Download Manager's Tree Structure....153
Making New Features Available....154
Hiding and Removing Features....155
Virus Scanning....156

LOGGING....157
Administrator Application Log Files....157
Recording Server Service Log Files....157
Event Log Files....157
Image Server Service Log Files....158
Image Server Audit Log Files....158
Image Import Service Log Files....158
Export Log Files....158
Integrity Checks and Possible Error Messages....159

VIDEO DEVICE DRIVERS....160
Updating Video Device Drivers....160

VIRUS SCANNING INFORMATION 162

PROTECTING DATABASES FROM CORRUPTION 163

USING 3 GB OPERATING SYSTEM VIRTUAL MEMORY 165

When Is 3 GB Switching Relevant? 165

What to Do 165

If Running Windows XP Professional or Windows Server 2003 166

If Running Windows 2008 Server or Windows Vista.....166

DAYLIGHT SAVING TIME 168

VIEWER 169

MONITOR..... 170

MATRIX MONITOR 171

ACCESS CLIENTS 172

Access Client Overview 172

Providing Access through a Remote Client or Smart Client 173

Providing Access through a PDA Client 173

Deciding Which Access Client to Use..... 173

Differences between Remote Client and Smart Client 174

Smart Client..... 175

Installation Options.....175

Download and Installation from Server 176

Installation from DVD 176

Silent Installation.....177

Remote Client 178

Accessing a Remote Client 178

PDA Client & Server 179
PDA Server Installation & Configuration Procedure 180
Installing IIS and .NET Framework 180
Installing the PDA Server 181
Verifying the PDA Server Installation 184
PDA Server Installation Troubleshooting 184

REMOVAL 186
Removing the Entire Surveillance System 186
Removing Individual Components 186
Removing the Surveillance Server Software 186
Removing Video Device Drivers 187
Removing the Download Manager 187
Removing the Viewer 187
Removing the Smart Client 187
Removing the PDA Software 187
PDA Server Removal Procedure 187
PDA Client Removal Procedure 188
Removing the Matrix Monitor Application 188
Removing Installation Files for End-User Features 189

GLOSSARY 190

INDEX 195

Introduction

Product Overview

With the purchase of XProtect Enterprise you have chosen an extremely powerful, flexible and intelligent surveillance solution.

XProtect Enterprise provides a state-of-the-art IP video surveillance system, supporting the widest choice of network cameras and video encoders, with the equipment connected to an office LAN or other TCP/IP network, such as the internet.

XProtect Enterprise is the perfect choice for large installations. XProtect Enterprise handles an unlimited number of cameras (up to 64 simultaneously used cameras per server), multiple servers and multiple sites. It is a top performance solution, well suited to the sophisticated high-end of the security market.

Several Targeted Components in One

XProtect Enterprise consists of a number of components, each targeted at specific tasks and user types:

- **The Administrator (see page 30):** The main application used by surveillance system administrators for configuring the XProtect Enterprise surveillance system server, upon installation or whenever configuration adjustments are required, e.g. when adding new cameras or users to the system.

- **The Recording Server (see page 68):** A vital part of the surveillance system; video streams are only transferred to XProtect Enterprise while the recording server is running. The recording server is automatically installed as a service (the Milestone Recording Server service), which will run in the background on the XProtect Enterprise surveillance system server. You are able to manage the service through the Recording Server Manager.

- **The Image Server (see page 139):** Handles access to the surveillance system for remote users logging in with the *Remote Client*, or *Smart Client* (see page 175), or *PDA Client*. The *Image Server* itself does not require separate hardware; it runs as a service on the surveillance system server. Surveillance system administrators handle *Image Server* configuration, including remote users' access rights, through the *Image Server Administrator* application.

- **The Download Manager (see page 152):** Lets surveillance system administrators manage which XProtect Enterprise-related features your organization's users will be able to access from a user-targeted welcome page on the surveillance system server.

- **The Remote Client** and **Smart Client (see page 172):** Choice of two types of remote access clients, each providing users with intuitive remote access to the surveillance system. The Remote Client and Smart Client let users view live video, play back recorded video, activate outputs, print and export evidence, etc. The Remote Client is accessed straight from the surveillance system server through an Internet Explorer browser. The extra feature-rich Smart Client should always be downloaded and installed on remote users' PCs.

- **The PDA Client/Server (see page 179):** Enable remote access to the XProtect Enterprise surveillance system via a PDA (Personal Digital Assistant; a hand-held computer device) with a wireless connection.

- **Milestone XProtect Matrix (see page 171):** Integrated product, enabling control of live camera views on remote computers for distributed viewing. Once configured, Matrix-triggered live video can be viewed in Smart Clients or on computers with the Matrix Monitor client application installed.

Updates

Milestone Systems regularly release service updates for our products, offering improved functionality and support for new devices.

If you are an XProtect Enterprise system administrator, it is recommended that you check the Milestone Systems website www.milestonesys.com for updates at regular intervals in order to make sure you are using the most recent version of XProtect Enterprise.

Requirements and Prerequisites

System Requirements

The following are *minimum* system requirements for running XProtect Enterprise and associated applications:

Surveillance System Server

Operating System	Microsoft® Windows® 2008 Server (32 bit or 64 bit*), Windows Server 2003 (32 bit or 64 bit*), Windows Vista® Business (32 bit or 64 bit*), Windows Vista Enterprise (32 bit or 64 bit*), Windows Vista Ultimate (32 bit or 64 bit*), Windows XP Professional (32 bit or 64 bit*).
CPU	Intel® Pentium® 4, 2.4 GHz or higher (Core™ 2 recommended).
RAM	Minimum 1 GB (2 GB or more recommended).
Network	Ethernet (1 Gbit recommended).
Graphics Adapter	AGP or PCI-Express, minimum 1024 x 768, 16 bit colors.
Hard Disk Type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster).
Hard Disk Space	Minimum 80 GB free (depends on number of cameras and recording settings).
Software	DirectX 9.0 or newer required to run Playback Viewer application. Microsoft .NET 1.1 Framework required to run Recording Server Manager. To run the PDA Server, the following is required: Internet Information Server (IIS) 5.1 or newer as well as Microsoft .NET Framework 2.0. Information about how to verify/install Microsoft .NET Framework and IIS versions is available on page 180.

* Running as a 32 bit service/application.

Tip: To check which DirectX version is installed on a computer, click *Start*, select *Run...*, and type `dxdiag`. When you click *OK*, the *DirectX Diagnostic Tool* window will open; version information is displayed near the bottom of its *System* tab. If the server requires a DirectX update, the latest versions of DirectX are available from http://www.microsoft.com/downloads/

Smart Client

Operating System	Microsoft Windows XP Professional (32 bit or 64 bit*) and Windows Server 2003 (32 bit or 64 bit*), Windows Vista Business (32 bit or 64 bit*), Windows Vista Enterprise (32 bit or 64 bit*) and Windows Vista Ultimate (32 bit or 64 bit*).
CPU	Intel Core2™ Duo, minimum 2.4 GHz or higher.

RAM	Minimum 512 MB (1 GB recommended for larger views, 1 GB recommended on Microsoft Windows Vista).
Network	Ethernet (100 Mbit or higher recommended).
Graphics Adapter	AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16 bit colors.
Hard Disk Space	Minimum 100 MB free.
Software	Microsoft .NET 2.0 Framework and DirectX 9.0 or newer.

* Running as a 32 bit service/application.

Remote Client

Operating System	Microsoft Windows XP Professional (32 bit or 64 bit*) and Windows Server 2003 (32 bit or 64 bit*), Windows Vista Business (32 bit or 64 bit*), Windows Vista Enterprise (32 bit or 64 bit*) and Windows Vista Ultimate (32 bit or 64 bit*). If running Windows Vista, the Remote Client must be added as a trusted site in your browser.
CPU	Intel Pentium 4, 2.4 GHz or higher.
RAM	Minimum 256 MB (512 MB recommended for larger views, 1 GB recommended on Microsoft Windows Vista).
Network	Ethernet (100 Mbit or higher recommended).
Graphics Adapter	AGP or PCI-Express, minimum 1024 x 768 (1280 x 1024 recommended), 16 bit colors.
Hard Disk Space	Minimum 10 MB free.
Software	DirectX 9.0 or newer.

* Running as a 32 bit service/application.

Tip: To check which DirectX version is installed on a computer, click *Start*, select *Run...*, and type dxdiag. When you click *OK*, the *DirectX Diagnostic Tool* window will open; version information is displayed near the bottom of its *System* tab. If the server requires a DirectX update, the latest versions of DirectX are available from http://www.microsoft.com/downloads/.

PDA Server

The *PDA Server* is typically installed on the surveillance system server; see the system requirements for the surveillance system server. Note, however, that to run the *PDA Server* the following is also required on the surveillance system server:

- Internet Information Services (IIS) 5.0 or later
- Microsoft .NET Framework 2.0.

Note that later versions of. Net Framework may also be present on the server. If .NET Framework 2.0 *as well as* one or more later versions are present on the server, Windows' default settings may

cause a later .NET Framework version to be used instead of .NET Framework 2.0. To verify/change which .NET Framework version is used, do the following:

1. Click *Start* and select *Control Panel*.
2. Click *Administrative Tools*.
3. Click *Internet Information Services*.
4. In the *Internet Information Services* window's left pane, locate and right-click the *Default Web Site* item:

Example only; content on your server may be different

5. In the resulting menu, select *Properties*. This will open the *Default Web Site Properties* dialog.
6. Select the dialog's *ASP.NET* tab. The .NET Framework in use will be indicated in the *ASP.NET version* field.
7. If required, change the *ASP.NET version* to *2.0.50727*.
8. Click *OK*.
9. Close the *Internet Information Services* and *Administrative Tools* windows if still open.

PDA Client

Operating System	Microsoft Windows Pocket PC 2003/2003 SE/Mobile 5.0.
CPU	Intel StrongARM or 100% compatible.
RAM	Minimum 32 MB.
Network	Ethernet (256 Kbit or higher recommended)
Graphics Adapter	Minimum 320 x 200, 16 bit colors.
Software	Microsoft Windows Pocket PC 2003/2003 SE/Mobile 5.0.

Matrix Monitor

Operating System	Microsoft Windows XP Professional (32 bit or 64 bit*) and Windows Server 2003 (32 bit or 64 bit*), Windows Vista Business (32 bit or 64 bit*), Windows Vista Enterprise (32 bit or 64 bit*) and Windows Vista Ultimate (32 bit or 64 bit*).
CPU	Intel Pentium 4, 2.4 GHz or higher.
RAM	Minimum 512 MB (1 GB recommended on Microsoft Windows Vista).

Network	Ethernet (100 Mbit or higher recommended).
Graphics Adapter	AAGP or PCI-Express, minimum 1024 x 768, 16 bit colors.
Hard Disk Space	Minimum 50 MB free.
Software	DirectX 9.0 or newer

* Running as a 32 bit service/application.

Important Port Numbers

XProtect Enterprise uses particular ports when communicating with other computers, cameras, etc.

What is a port? A port is a logical endpoint for data traffic. Networks use different ports for different types of data traffic. Therefore it is sometimes, but not always, necessary to specify which port to use for particular data communication. Most ports are used automatically based on the types of data included in the communication. On TCP/IP networks, port numbers range from 0 to 65536, but only ports 0 to 1024 are reserved for particular purposes. For example, port 80 is used for HTTP traffic which is used when viewing web pages.

When using XProtect Enterprise, make sure that the following ports are open for data traffic on your network:

- **Port 20 and 21 (inbound and outbound):** Used for FTP traffic. FTP (File Transfer Protocol) is a standard for exchanging files across networks. FTP uses the TCP/IP standards for data transfer, and is often used for uploading or downloading files to and from servers.

- **Port 25 (inbound and outbound):** Used for SMTP traffic. SMTP (Simple Mail Transfer Protocol) is a standard for sending e-mail messages between servers. This port should be open since, depending on configuration, some cameras may send images to the surveillance system server via e-mail.

- **Port 80 (inbound and outbound):** Used for HTTP traffic between the surveillance server and cameras, Remote Clients and/or Smart Clients, and the default communication port for the surveillance system's Image Server. HTTP (Hypertext Transfer Protocol) is a standard for exchanging files across networks; widely used for formatting and transmission of data on the world wide web.

- **Port 1024 and above (outbound only):** Used for HTTP traffic between cameras and the surveillance server.

- Any other port numbers you may have selected to use, for example if you have changed the *Image Server*'s port from its default port number (80) to another port number.

Tip: Consult the administrator of your organization's firewall if in doubt about how to open ports for traffic.

If you wish to install, configure and run XProtect Enterprise on a Windows Vista computer, it is very important that you have administrator rights. If you only have standard user rights, you will not be able to configure the software or stop and start the Recording Server service. However, you are still able to view live and recorded video via the Smart Client.

These restrictions are a part of the User Account Control, a security component in Windows Vista. Note, however, that it is possible to disable the User Account Control. For more information visit www.microsoft.com, and search for Vista User Account Control or similar.

Time Server Recommended

All images are time-stamped by XProtect Enterprise upon reception, but since cameras are separate units which may have separate timing devices, power supplies, etc., camera time and XProtect Enterprise system time may not correspond fully, and this may occasionally lead to confusion.

If supported by your cameras, we thus recommend you auto-synchronize camera and system time through a time server for consistent synchronization.

For information about configuring a time server searching www.microsoft.com for *time server*, *time service*, or similar.

Administrators' Getting Started Checklist

This chapter outlines the tasks typically involved in setting up a working XProtect Enterprise system. The information in this chapter is primarily aimed at system administrators.

Note that although information in this chapter is presented as a checklist, a completed checklist does not in itself guarantee that the XProtect Enterprise system will match the exact needs of your organization. To make the system match the needs of your organization, it is highly recommended that you monitor and adjust the system once it is running.

For example, it is often a very good idea to spend time on testing and adjusting the motion detection sensitivity settings for individual cameras under different physical conditions (day/night, windy/calm, etc.) once the system is running. The setup of events and associated actions (see About Input, Events & Output … on page 84) is another example of configuration which depends entirely on your organization's needs.

☑ You may check the boxes in this checklist as you go along.

☐ **Verify Initial Configuration of Devices**. Make sure the devices (IP network cameras or IP video encoders) you are going to use are configured with IP addresses, passwords, etc. as specified by the manufacturer.

Such initial configuration is required in order to be able to connect the devices to the network and the XProtect Enterprise solution.

☐ **Register software and obtain Device License Keys**. You must have a Device License Key (DLK) for each device (IP network camera or IP video server) to be used with the XProtect Enterprise solution.

You obtain DLKs as part of the software registration process on the Milestone Systems website, www.milestonesys.com:

- Click the *Software Registration* link.
- Log in to the online registration system. If you do not yet have a login, click the *New To The System?* link, and follow the instructions. When ready, log in using the registered e-mail address and password. The DLKs will be e-mailed to the e-mail address specified in your login, so it is a good idea to use a single e-mail account for all persons who should be able to retrieve DLKs.
- If you have not yet registered your SLC (Software License Code; listed on your product license sheet), do so by clicking the *Add SLC* link and completing the SLC registration steps before proceeding.
- When ready, click the link representing the SLC.
- For **each** device required on your system, click the *Add new MAC* link and specify the device's MAC address and a description. The MAC address is a 12 digit hexadecimal (example: 0123456789AF), referred to as a *serial number* by some vendors. For information about how to find the MAC address for a specific device, refer to the manual for the device in question.
- For video encoder devices, specify the number of cameras to be used with the device. Note that you are allowed to install only the number of cameras listed on your product license sheet. For example, a fully used four-port video server counts as four cameras

even though the cameras are connected through a single device—therefore a fully used four-port video server will use four licenses.

- Click *Submit*. The device is added to a list of devices under your SLC.
- If more devices are required, click the *Add New MAC* link and repeat the process.
- When ready, click the *Get DLKs by e-mail* link to have DLKs for all the devices registered under your SLC e-mailed to you.

☐ **Install XProtect Enterprise** (see *Installation* on page 24).

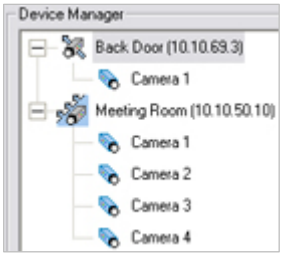
☐ **Import Device License Keys** (see *How to Import Device License Keys (DLKs)* on page 35).

☐ **Add IP Devices** (see *How to Add a device* on page 36). In XProtect Enterprise you do not have to worry about having to add individual cameras to the system. This is because cameras area connected to IP devices, so once you have added the required devices to your XProtect Enterprise system, all cameras connected to the devices are connected to the system as well.

☐ **Configure Cameras on XProtect Enterprise**. You are able to specify a wide variety of settings for each camera connected to the XProtect Enterprise system.

Your entry point for configuring cameras is the *Administrator* window, the main window in XProtect Enterprise's *Administrator* application (see page 30).

To configure a camera, first select the required device in the *Administrator* window's *Device Manager* section, then click the plus sign next to the device to view a list of cameras attached to the device, as illustrated in the following:



Select the required camera from the list, and click the *Administrator* window's *Settings* button. This will open the *Camera Settings for [Device Name] [Camera Name]* window, in which you are able to specify settings for the camera in question.

Settings include the highly important motion detection sensitivity settings. They also include PTZ (Pan/Tilt/Zoom) preset position settings for any PTZ cameras supporting preset positions. The *Camera Settings for [Device Name] [Camera Name]* window is described in detail on page 43.

☐ **Configure XProtect Enterprise's General Settings**. The *Administrator* application's *General Settings* window lets you configure a number of important settings related to user rights, logging, e-mail and SMS accounts, etc.

The *General Settings* window is described in detail on page 76.

☐ **Configure Scheduling**. You may want some cameras to be transferring video to XProtect Enterprise at all times, whereas you may want other cameras to transfer video only within specific periods of time, or when specific events occur. With XProtect Enterprise's scheduling feature, you are able to specify when each camera should transfer video. You are also able to specify whether alerts should be triggered if motion is detected during specific periods of time.

For PTZ cameras with patrolling (the automatic movement of a camera between several preset positions), you are furthermore able to specify whether any specific patrol schemes should be used during specific periods of time.

You configure scheduling in the *Administrator* application's *Camera/Alert Scheduler* window, described in detail on page 71.

☐ **Configure Archiving**. By default, video received from cameras is stored by XProtect Enterprise in a database for each camera. However, the camera databases are each capable of containing a maximum of 40 GB or 600,000 records before the oldest records are deleted.

By using XProtect Enterprise's archiving feature, you are able to overcome these limitations by automatically moving the contents of camera databases to specified archiving locations one or more times every day. With archiving the amount of records you will be able to store will thus be limited only by your available hardware storage capacity.

By using archiving, you will also be able to back up archived records on backup media of your choice, using your preferred backup software.

Archiving is described in detail on page 125.

☐ **Configure the Image Server.** The Image Server is the service handling Remote Client and Smart Client access to the XProtect Enterprise system.

Remote Clients (see separate manual) and Smart Clients (see separate manual) are included in your XProtect Enterprise license, and provide flexible, client/server based, remote access to the XProtect Enterprise system, with viewing live or recordings from multiple servers simultaneously. If you are going to use Remote Clients or Smart Clients, configuring the Image Server is a prerequisite. Configuration includes specifying whether the *Image Server* should be accessible from the internet, specifying user rights, etc.

If the PDA Server front end (see the following) is installed, the Image Server also handles user rights, etc. for PDA Client users.

You configure the Image Server through the *Image Server Administrator* window, described in detail on page 139.

☐ **Configure the Download Manager.** The Download Manager lets you manage which XProtect Enterprise-related features your organization's users will be able to access from a user-targeted welcome page on the surveillance system server. Such features include the highly important access clients, additional language versions, etc.

Tip: The Download Manager comes with a default configuration ensuring that users get access to Smart Clients (see page 175) and Remote Clients (see page 178) on the welcome page without you having to configure anything.

Read more about the Download Manager, the welcome page, users' language options, etc. on page 152.

☐ **(Optional) Install and Configure the *PDA server*.** The *PDA Server* enables *PDA Client* remote access to the XProtect Enterprise system. Read more on page 179.

☐ **(Optional) Configure *Matrix*:** Milestone XProtect Matrix is an integrated product that allows distributed viewing of video from any camera on any monitor on a network operating with XProtect Enterprise. Read more on page 135.

Installation

Microsoft® Windows® Vista® Information

If you wish to install, configure and run XProtect Enterprise on a Windows Vista computer, it is important that you have administrator rights. If you only have standard user rights, you will not be able to configure the software.

These restrictions are a part of the User Account Control, a security component in Windows Vista. Note, however, that it is possible to disable the User Account Control. For more information, search www.microsoft.com for *Vista User Account Control* or similar.

Installing the Server Software

If upgrading from a previous version, make sure you read the upgrade information on page 25 before you begin upgrading.

Note: Do not install XProtect Enterprise on a mounted drive (i.e. a drive attached to an empty folder on an NTFS (NT File System) volume, with a label or name instead of a drive letter). If using mounted drives, critical system features may not work as intended; you will, for example, not receive any warnings if the system runs out of disk space.

Prerequisites: Shut down any existing Milestone software.

1. Insert the XProtect Enterprise software DVD, wait for a short while, select required language, then click the Milestone XProtect Enterprise installation link.

   Alternatively, if you are installing a version downloaded from the internet, run the downloaded installation file from the location you have saved it to.

   Tip: Depending on your security settings, you may receive one or more security warnings (*Do you want to run or save this file? Do you want to run this software?* or similar). When this is the case, click the *Run* button.

2. When the installation wizard starts, click *Next* to continue.

3. Read and accept the End User License Agreement, then click *Next*.

4. If an earlier XProtect Enterprise version (6.0a or later) is present on the server, you will be asked to accept that it is automatically removed during installation of the new version. The automatic removal will not delete any existing recordings or configuration. If asked, we recommend answering *Yes*, since this will ensure that old versions will not interfere with your new version. XProtect Enterprise versions earlier than 6.0 must be removed manually before installing the new version, see Upgrading from a Previous Version on page 25.

5. Select *Typical* installation (advanced users can select *Custom* installation, and choose which features to install and where to install them).

6. Select the *Install licensed Version* option, and specify your user name, organization, and Software License Code (SLC; printed on your Product License Sheet). When ready, click *Next*.

7. Click the *Install* button to begin the software installation. During the process, all the necessary components will be installed one after the other.

    - XProtect Enterprise's *Administrator* window may appear on your screen during installation. When this is the case, the window will automatically close again after a short while.

    - If a *Status Information* window appears on your screen during installation, click its *OK* button (the window simply provides a summary of your installation).

8. Click *Finish* on the last step to complete the installation.

When installation is complete, you can begin configuring your XProtect Enterprise solution: Double-click the *Administrator* desktop shortcut or select *Start > All Programs > Milestone XProtect Enterprise > Administrator* to open the Administrator window.

Tip: If you want to make additional language versions of the Smart Client and Remote Client (such as Spanish, French, or Japanese versions) available to your organization's users, you can quickly do this once you have installed XProtect Enterprise. See more in the description of the Download Manager on page 152.

Upgrading from a Previous Version

Upgrading XProtect Enterprise is an easy task, and you need not worry about spending hours reconfiguring your software.

The following information applies if upgrading from one XProtect Enterprise version to another as well as if upgrading to XProtect Enterprise from a lower product in the XProtect product portfolio.

Prerequisites

- Take note of your SLC (Software License Code). The SLC will change when the software version number changes.

- If your SLC has changed, so have your DLKs (Device License Keys). Go to the Milestone website, www.milestonesys.com, and log in to the Software Registration Service Center. Under the properties for your license, click the *Get DLKs by e-mail* link. When you receive the .dlk file, save it on the computer running the XProtect Enterprise server.

- If you do not already have the new XProtect Enterprise new, go to www.milestonesys.com, and download the most current version which you are allowed to install with your SLC.

Backing Up Your Current Configuration

It is generally a good idea to make regular backups of your server configuration as a disaster recovery measure. Upgrading your server is no exception. While it is rare to lose your configuration (cameras, schedules, views, etc), it *can* happen under certain circumstances. Luckily, it takes only a minute to back up your existing configuration:

1. Create a folder called *Backup* on the desktop of your XProtect Enterprise server, on a network drive, or on removable media.

2. Open *My Computer*, and navigate to C:\Program Files\Milestone\Milestone Surveillance.

3. Copy the following files and folders into your *Backup* folder:
    - All configuration (.ini) files
    - All scheduling (.sch) files
    - The file *users.txt* (not found in most installations)
    - The folder *SmartClientViewGroups* and all of its content
    - The folder *RemoteClientViewGroup*s and all of its content

Note that some of the folders may not exist if upgrading from old software versions.

Removing the Current Version

XProtect Enterprise versions 6.0a or later can automatically be removed during installation of the new version. When installing the new version, simply answer *Yes* if asked if you accept such automatic removal. The automatic removal will not delete any existing recordings or configuration.

XProtect Enterprise versions older than 6.0 as well as lower products in the XProtect product portfolio must be removed manually before installing the new version. Manually removing the old version involves removing two components on the server. Removing these components will not remove your configuration files.

1. From Windows' *Start* menu, select *Control Panel* > *Add or Remove Programs*.
2. Remove Milestone XProtect Enterprise (or the lower XProtect product).
3. When asked if you want to remove database files or registry settings, you should normally not select any of the check boxes.

    You may choose to remove database files if you wish, but removing registry settings may mean that the new software version will not be able to utilize the existing configuration.
4. Remove Video Device Driver/Pack Vx.x (where x.x refers to the version number).

Installing the New Version

Once the old version of the software is removed, you can run the installation file for the new software version. Select the installation options that best fit your needs.

There are some recent software changes that you should be aware of:

- It is now possible to install the software as a service, and as of XProtect Enterprise 6.5 this is the only option since the Monitor application has been discontinued. When the software runs as a service, the Recording Server runs as a background process, and any viewing either locally or remotely will be done through either a Smart Client (see page 175), through a Remote Client (see page 178), or through the PDA Client/PDA Server solution(see page 179).
- The HTTP Server/Realtime Feed Server (very basic alternative to the Smart Client/Remote Client) can only be used when the software is installed as an application. Since installing as an application is no longer possible in current XProtect Enterprise versions, the HTTP Server and Realtime Feed Server have been discontinued. Use the much superior Smart Client or Remote Client instead.

- XProtect Enterprise's *Administrator* window (see page 30) may appear on your screen during installation. When this is the case, the window will automatically close again after a short while.

- In the most recent software version, a Download Manager (see page 152) is introduced, and you will have the option of opening the Download Manager during installation. The Download Manager is used for managing which features your organization's users will be able to access from a targeted welcome page on the surveillance system server. You can open the Download Manager if you like, but you can just as easily make changes through the Download Manager once installation is completed.

Restoring a Configuration Backup (if Required)

If for some reason after installing the new software version you have lost your old configuration, you can easily restore your configuration, provided you have created a backup of your configuration prior to upgrading the software:

1. Drag and drop the backed-up configuration files and folders into the new installation directory, which by default is still C:\Program Files\Milestone\Milestone Surveillance\.

2. When asked if you wish to overwrite the existing files, click *Yes*.

3. Restart your server.

Updating Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to an XProtect Enterprise system.

Video device drivers are installed automatically during the initial installation of your XProtect Enterprise system. However, new versions of the video device drivers, so-called Device Packs, are released and made available for free on the Milestone website from time to time.

We therefore recommend that you visit the Milestone website (www.milestonesys.com; look under *Support* > *Downloads*) and download the latest Device Pack.

Upgrading Smart Clients

Smart Client users should now remove their old Smart Client versions and install the new one:

1. On the required computers, open Windows' *Add or Remove Programs* dialog (*Start* > *Control Panel* > *Add or Remove Programs*).

2. In the *Add or Remove Programs* dialog, select the Milestone XProtect Smart Client entry, and click the *Remove* button. A wizard window will open. Follow the wizard's steps, and click *Finish* when ready.

3. Now open a browser and connect to XProtect Enterprise at the following address:

   http://[IP address or hostname of server]:[Image Server port number; default is 80]

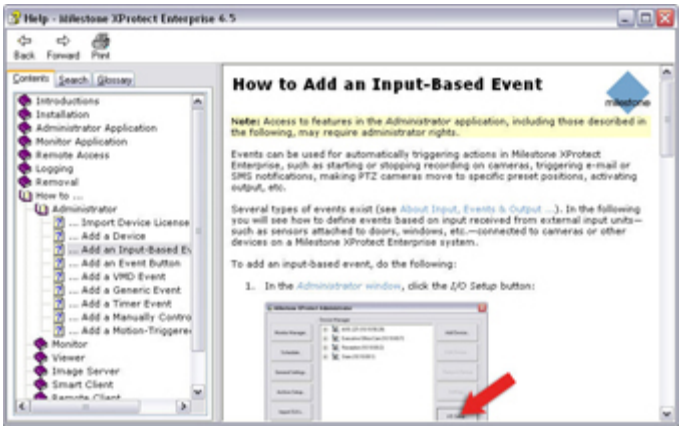
   Example: http://123.123.123.123:80

4. From the welcome page that appears, download and install the latest Smart Client version.

5. If required, download and install any Smart Client plugins needed.

Using the Built-in Help System

To use XProtect Enterprise's built-in help system, simply press the F1 key on your keyboard whenever you are working with the *Administrator* application or *Image Server Administrator*.



When you press F1, the help system will open in a separate window, allowing you to easily switch between help and XProtect Enterprise itself.

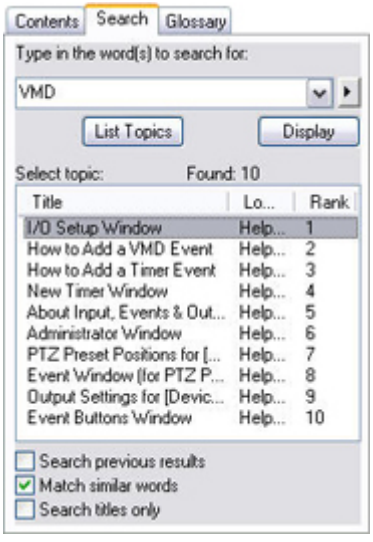
The help system is context sensitive. This means that when you press F1 for help while working in a particular window or with a particular task, the help system automatically displays the help topic describing that window or task.

Navigating the Built-in Help System

Even though the help system initially takes you to a topic describing the window you are working in, you are always able to freely navigate between the help system's contents. To do this, simply use the help window's three tabs, *Contents*, *Search* and *Glossary,* or use the links inside the help topics.

Contents Tab

The *Contents* tab lets you navigate the help system based on a tree structure. Many users will be familiar with this type of navigation from, for example, Windows Explorer.



Search Tab

The *Search* tab lets you search for help topics containing particular terms of interest. For example, you can search for the term *zoom*, and every help topic containing the term *zoom* will be listed in the search results. Clicking a help topic title in the search results list will open the required topic.

The *Search* tab contains a number of advanced search features; among these are the ability to quickly run previous searches, the ability to search topic titles only as well as the ability to display search results ranked according to presumed relevance.

Glossary Tab

What do abbreviations such as DLK, PTZ or VMD stand for? The *Glossary* tab in the help window's navigation pane provides a glossary of common surveillance and network-related terms. Simply select a term to view a corresponding definition in the small window below the list of terms.

Links in Help Topics

The actual content of each help topic is displayed in the right pane of the help window. Help topic texts may contain various types of links, notably so-called expanding drop-down links.

Clicking an expanding drop-down link will display detailed information. The detailed information will be displayed immediately below the link itself; the content on the page simply expands. Expanding drop-down links thus help save space.

Tip: If you wish to quickly collapse all texts from expanding drop-down links in a help topic, simply click the title of the topic on the help system's *Contents* tab.

Printing Help Topics

To print a help topic, navigate to the required topic and click the help window's *Print* button.

When you click the *Print* button, a dialog box may ask you whether you wish to print the selected topic only or all topics under the selected heading. When this is the case, select *Print the selected topic* and click *OK*.

When printing a selected help topic, the topic will be printed as you see it on your screen. Therefore, if a topic contains expanding drop-down links (see *Links in Help Topics* in the previous), click each required drop-down link to display the text in order for it to be included in your printout. This allows you to create targeted printouts, containing exactly the amount of information you require.

The Administrator Application

Administrator Login Window

For users without administrator rights, access to certain features in XProtect Enterprise may in some organizations have been restricted. When this is the case, you will be asked to specify the administrator password in the *Administrator Login* window in order to get access to the restricted features.

You will only be asked to specify the administrator password when you open the *Administrator* application, by selecting it from Windows' *Start* menu or by clicking the *Administrator* shortcut on the desktop. This will only be the case when access to the *Administrator* application has been password-protected.

Administrator Window

The *Administrator* window, the main window in the *Administrator* application, is used by the surveillance system administrator for configuring XProtect Enterprise upon installation or whenever configuration adjustments are required, e.g. when adding new cameras to the system.

You access the *Administrator* application by selecting it from Window's *Start* menu or by clicking the *Administrator* shortcut on the desktop. Access to the *Administrator* application may be password protected, in which case you will be asked to provide the administrator password in the *Administrator Login* window (see above).

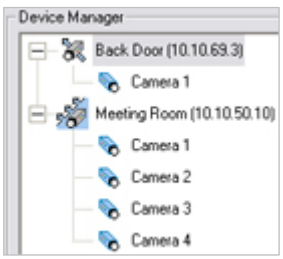
Administrator desktop shortcut

IMPORTANT: Changes you make in the *Administrator* application are not applied on your surveillance system until you exit the *Administrator* application. This allows you to try out various settings before making them take effect.

Tip: Clicking the icon in the left corner of the *Administrator* window's title bar, gives you access to a small menu. Selecting *About Adm ...* from the menu will display a dialog with your system's version number and Software License Code. This is valuable information, should you ever need to contact product support.

Device Manager Section

The *Device Manager* section—located in the middle of the Administrator window—lists all added devices and attached cameras. The Device Manager section thus provides you with an overview of your surveillance system.



Until you have added devices, the *Device Manager* section will be empty. The illustration to the right shows a detail from the *Administrator* window's *Device Manager* section—two devices have been added; the first device has a single camera attached, whereas the second device has four cameras attached.

Adding Devices

You add devices through an intuitive Device Setup Wizard, available by clicking the Administrator window's *Add Device* button (see also How to Add a Device on page 36). When devices have been added, they will be listed in the Device Manager section. Clicking the plus sign ⊞ next to a device in the Device Manager section will list cameras attached to the device.

Editing Settings for Devices

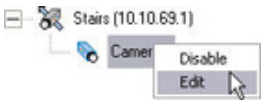
To edit settings for a device listed in the *Device Manager* section, select the device, then click the *Edit device...* button to open the *Edit device settings* window (see page 38).

Editing Settings for Cameras

To edit the settings for a camera listed in the Device Manager section, click the plus sign ⊞ next to the device to which the camera is attached, select the required camera, then click the Settings button to open the *Camera Settings for [Device name] [Camera Name]* window (see page 43).

Renaming Cameras

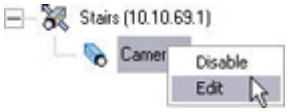
To rename a camera, right-click the camera name in question, then select Edit from the menu that appears. This will open the *Camera Name and Number* window (see page 64), in which you are able to overwrite the existing camera name with a new one.



Assigning Shortcut Numbers to Cameras

Users of the Smart Client (see page 175) can take advantage of a range of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such keyboard shortcuts include numbers, which are used to identify each camera. Shortcut numbers must be unique for each camera.

To assign a shortcut number to a camera, right-click the camera name in question, then select Edit from the menu that appears. This will open the *Camera Name and Number* window (see page 64), in which you are able to specify a shortcut number to be used with the camera.



Note: Camera shortcut numbers are only used in the *Smart Client* (see page 175). In other applications, such as the *Remote Client* (see page 178), the camera shortcuts cannot be used.

Tip: More information about using the keyboard shortcuts is available in the documentation for the Smart Client.

Editing Settings for Audio Sources

To edit the settings for an audio source (that is a microphone or a speaker) listed in the Device Manager section, click the plus sign next to the device to which the audio source is attached, select the required audio source, and then click the Settings button to open the *Microphone Settings* window (see page 67) or the *Speaker Settings* window (see page 67).

IMPORTANT: The use of microphones will impact the database capacity for storing video; see Important Information (on page 66) about Using Audio for more information.

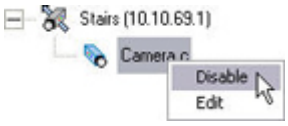
Disabling/Enabling Cameras and Audio Sources

Individual cameras and audio sources listed in the *Device Manager* section are by default disabled, meaning that video from cameras and audio from attached microphones is by default transferred to

XProtect Enterprise—provided that the cameras are marked as *online* in the *Camera/Alert Scheduler* Window (also default) – see page 71 .

Note: On some devices, audio can also be enabled/disabled on the device itself, typically through the device's own configuration web page. If audio on a device does not work after enabling it in the *Administrator* application, you should thus verify whether the problem may be due to audio being disabled on the device itself.

If required, you can disable individual cameras and audio sources listed in the *Device Manager* section. When a camera or audio source is disabled, no video/audio will be transferred from the camera/audio source to XProtect Enterprise. To disable a camera or audio source, right-click the required camera or audio source in the *Device Manager* section, then select *Disable*.



When a camera or audio source is disabled, it will be indicated as follows:

To enable a previously disabled camera or audio source, simply right-click the required camera or audio source in the *Device Manager* section, then select *Enable*:

Tip: Individual cameras can also be disabled/enabled in the *Camera Settings for [Device Name] [Camera Name]* Window (see page 43). Individual audio sources can also be disabled/enabled in the *Microphone Settings* window (see page 67) and the *Speaker Settings* window (see page 67).

Administrator Window's Buttons

Button	Description
Service Manager...	Opens the *Service Manager* window (see page 70), which lets you pause/resume the *Milestone Recording Server* service. Pausing the service is necessary in order to access some features, for example configuration of PTZ (Pan/Tilt/Zoom) cameras. **IMPORTANT:** While the service is paused, no video or audio will be recorded.
Scheduler...	Opens the *Camera/Alert Scheduler* window (see page 71), in which you specify online periods for each camera. You are also able to specify if cameras should go online when specific events occur (e.g. when a door is opened), and if e-mail or sound alerts should be used if motion is detected during specific periods of time (e.g. during working hours). If using PTZ cameras with patrolling, you are furthermore able to specify if certain patrol schemes should be used during specific periods of time. **Tip:** By default, all cameras are online at all times. You will only need to modify scheduler settings if you require cameras to be online only at specific times or events, or if you want to use specific alerts or PTZ patrol schemes.

Button	Description
General Settings...	Opens the *General Settings* window (see page 76), in which you are able to specify a number of settings related to: • Administrator password • User rights for the *Administrator* application • Milestone XProtect Central settings (if using the Milestone XProtect Central centralized monitoring solution in connection with XProtect Enterprise) • PTZ patrolling pause time out (if using PTZ cameras with patrolling) • E-mail settings (for alerts sent via e-mail) • SMS settings (for alerts sent via SMS) • Log file settings • Other advanced settings
Archive Setup...	Opens the *Archive setup* window (see page 130), in which you specify XProtect Enterprise's archiving settings. Archiving lets you keep recordings for as long as required, limited only be the available hardware storage capacity.
Import DLKs...	Lets you import all required Device License Keys (DLKs) in one go, thus avoiding the need to specify each DLK manually when adding devices. See also *How to Import Device License Keys* on page 35.
Matrix...	Lets you access Matrix configuration (see page 135). Matrix is an integrated product for forcing video from any camera to any monitor on a network operating with XProtect Enterprise.
Transact...	**Note:** The *Transact* button is not functional. If Milestone XProtect Transact (add-on product for handling loss prevention through video evidence combined with time-linked POS or ATM transaction data) is installed on the server, use Windows' *Start* menu or the *Transact Administrator* desktop shortcut to access the Transact Administrator. Use with Milestone XProtect Transact versions earlier than 2.1 is not supported.
Add Device...	Starts the *Device Setup Wizard*, which guides you through the process of adding a new device. See also *How to Add a Device* on page 36.
Edit Device...	When you have selected a device in the *Administrator* window's *Device Manager* section, clicking the *Edit Device...* button lets you edit settings for the selected device in the *Edit device settings* window (see page 38).
Remove Device	Lets you remove a device selected in the *Administrator* window's *Device Manager* section. In order to prevent accidental removal of devices, you will be asked to confirm that you want to remove the device.
Settings...	Lets you specify settings for a selected camera or audio source:

Button	Description
	• *Cameras*: When you have selected a camera in the *Administrator* window's *Device Manager* section, clicking the *Settings* button will open the *Camera Settings for [Device Name] [Camera Name]...* window (see page 43), in which you specify camera settings. • *Audio sources*: When you have selected a microphone or a speaker in the *Administrator* window's *Device Manager* section, clicking the *Settings* button will open the *Microphone Settings* window (see page 67) or the *Speaker Settings* window (see page 67), in which you can enable/disable the microphone or speaker and change its name if required.
I/O Setup...	Opens the *I/O Setup* window (see page 86), in which you are able to define events based on input events (for example when a door sensor detects that a door is opened) and VMD (Video Motion Detection). The *I/O Setup* window also lets you specify output (e.g. a siren). When defined, events can be used for a variety of purposes. For example, an input event can be used for triggering output, for starting a particular camera, and for triggering that an e-mail or SMS message is sent to a particular user, notifying the user of the recorded event. See also the description of the *I/O Control...* button below.
Event Buttons...	Opens the *Event Buttons* window (see page 96), in which you are able to define events for use on event buttons. Event buttons can be used in the Smart Client for manually triggering events.
Generic Events...	Opens the *Generic Events* window (see page 100), in which you are able to define events based on input from external sources using the TCP and UDP protocols.
I/O Control...	Opens the *I/O Control* window (see page 105) where you are able to attach outputs to input events. This way you can, for example, define that a siren should sound when a sensor detects that a door is opened.
Exit	Closes the *Administrator* application.

Tip: Clicking the icon in the left corner of the *Administrator* window's title bar, gives you access to a small menu. Selecting *About Adm ...* from the menu will display a dialog with your system's version number and software license code; this is valuable information, should you ever need to contact product support.

Device License Keys (DLKs)

How to Import Device License Keys

You must have a Device License Key (DLK) for every device (IP network camera or IP video server) installed on your XProtect Enterprise surveillance system.

Remember that you are allowed to install and use only the number of cameras listed on your organization's license sheet; regardless of you number of available DLKs. For example, a fully used four-port video encoder counts as four cameras even though the cameras are connected through a single device—therefore a fully used four-port video encoder will use four licenses.

System administrators obtain DLKs as part of the software registration process on the Milestone website, www.milestonesys.com. Upon registration, DLKs are sent to system administrators via e-mail.

You are able to specify each DLK manually when adding a device (see page 36) through the D*evice Setup Wizard*, available by clicking the Add Device... button in the Administrator window (see page 30). However, you can avoid having to specify each DLK manually by using the following procedure to import all received DLKs into XProtect Enterprise in one go:

Prerequisites: The DLKs, received in a .dlk file, must have been saved at a location accessible by the surveillance server, for example on a network drive or on a USB stick.

1. Open the *Administrator* window (see page 30).

2. In the *Administrator* window, click the *Import DLKs...* button.Browse to the location at which you have saved the received .dlk file.

3. Select the file, and click *Open*. All DLKs are now automatically imported, and the relevant DLK will automatically appear when you add a device through the *Device Setup Wizard*.

IP Device Administration

How to Add a Device

In XProtect Enterprise you add devices (IP video camera devices, IP video encoder devices or digital video recorder devices (DVR devices)) rather than actual cameras. This is because devices have their own IP addresses—sometimes also host names for easier identification—on the network. Being IP-based, XProtect Enterprise primarily identifies units on the surveillance system based on their IP addresses or host names.

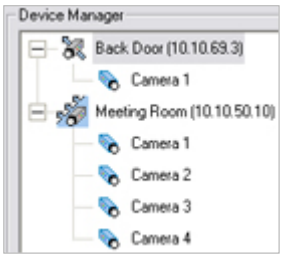
Example of IP address: 123.123.123.123. Example of hostname: OurDevice.

Even though each device has its own IP address/host name, several cameras can be attached to a single device and thus share the same IP address/host name. This is typically the case with cameras attached to video encoder devices or DVR devices.

You can of course configure and use each camera individually, even when several cameras are attached to a single device.

In addition to IP video camera devices, IP video encoder devices and DVR devices it is possible to add a number of dedicated I/O (input/output) devices to XProtect Enterprise. When such I/O devices are added, they can be used in events-based system setup in the same way as a camera. For more information about using I/O devices, see Using Dedicated I/O Devices on page 85). For information about which I/O devices are supported, refer to the release note.

Once a device is added in XProtect Enterprise, any cameras attached to the device are automatically recognized by the software, and listed in the *Administrator* window's *Device Manager* section



The illustration to the right shows a detail from the *Administrator* window's *Device Manager* section—two devices have been added; the first device has a single camera attached, whereas the second device has four cameras attached.

To add a device, use the following procedure:

Prerequisites: You must have configured IP address, password, etc. on the device itself, as described by the manufacturer.

1. Open the *Administrator* window (see page 30).

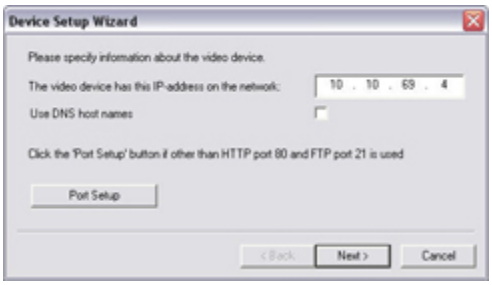
2. In the *Administrator* window, click the *Add Device...* button. This will start the *Device Setup Wizard*.

3. On the first step of the wizard, identify the required device, either by

   - Typing the IP address of the device (to jump to the next IP address segment in the field, press SPACE on your keyboard).

     - or -

   - Typing the DNS host name of the device. This requires that you select the *Use DNS host names* box


Device Setup Wizard
Please specify information about the video device.
The video device has this IP-address on the network:
10 . 10 . 69 . 4
Use DNS host names
Click the 'Port Setup' button if other than HTTP port 80 and FTP port 21 is used
Port Setup
< Back
Next >
Cancel

Specifying the IP address of a device

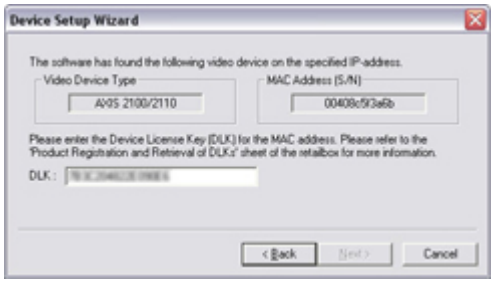
Note: By default, HTTP port 80 and FTP port 21 will be used for the device. If the device you are adding uses other port numbers, click the *Port Setup* button and specify required port numbers. The need for specifying different ports may often apply if the device is located behind a NAT-enabled router or a firewall. When this is the case, also remember to configure the router/firewall so it maps the ports and IP address used by the device.

When ready, click *Next* to go to the second step of the wizard.

4. If a password is used for the device, type the password for the device's administrator account (called the "admin" or "root" account on some devices). Leave the *Autodetect Device* option selected. Then click *Next*.

Tip: If you are in doubt about which administrator account to use for a device, look in the Device Pack Release Notes, available from the *Downloads* section of the Milestone website, www.milestonesys.com.

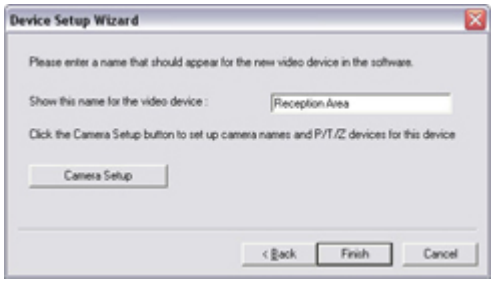
5. When the device has been detected, type the Device License Key (DLK) for the device in the *DLK* field.


Device Setup Wizard
The software has found the following video device on the specified IP-address.
Video Device Type
AXIS 2100/2110
MAC Address (S/N)
00408c5f3a6b
Please enter the Device License Key (DLK) for the MAC address. Please refer to the 'Product Registration and Retrieval of DLK's' sheet of the retailbox for more information.
DLK:
< Back
Next >
Cancel

Tip: If you have imported DLKs (see How to Import Device License Keys on page 35), the *DLK* field will already be filled with the DLK for the device.

Click *Next*.

6. Assign a unique and descriptive name to the device.


Device Setup Wizard
Please enter a name that should appear for the new video device in the software.
Show this name for the video device:
Reception Area
Click the Camera Setup button to set up camera names and P/T/Z devices for this device
Camera Setup
< Back
Finish
Cancel

Upon completion of the wizard, the name will be used when listing devices and associated cameras in the *Administrator* window's *Device Manager* section. The name may, for example, refer to the physical location of the camera(s) attached to the device.

Tip: You may click the *Camera Setup* button to access the *Camera Settings for [Device Name]* window (see page 40), in which you are able to specify certain settings related to camera name and PTZ control. The latter requires that the camera is a PTZ (Pan/tilt/Zoom) camera.

7. Click *Finish*.

8. The device will be listed in the *Administrator* window's *Device Manager* section. To view a list of cameras attached to the device, click the plus sign ⊞ next to the device name.

Tip: In the Administrator application's *Device Manager* section (the white area in the middle of the window), cameras are listed for each device with default names, such as *Camera 1*, etc. If you want to change the name of a camera, click the plus sign next to the required device, right-click the camera name in question, then select *Edit* from the menu that appears.

Tip: Individual cameras listed in the *Device Manager* section are by default enabled, meaning that video from the cameras is by default transferred to XProtect Enterprise—provided that the cameras are marked as *online* in the *Camera/Alert Scheduler* Window (also default) – see page 71. If required, you can disable a camera listed in the *Device Manager* section by right-clicking the name of the camera in question. See more information under *Administrator* window (see page 30).

Edit Device Settings Window

The *Edit device settings* window lets you edit the settings of an already installed device.

To access the *Edit device settings* window (see page 38), select the required device in the *Administrator* window's (see page 30) *Device Manager* section, and click the *Edit Device...* button.

The *Edit device settings* window is divided into two sections:

Identify Video Device Section

The Identify Video Device section contains the following fields, buttons, etc.:

Field, Button, ...	Description
Device Type	Select required device type from list. XProtect Enterprise is able to automatically detect device type as well as serial number, provided the IP address/hostname and password of the device have been specified in the *IP-address/DNS Host Name* and *Root Password* fields: Simply click the *Detect Device* button to auto-detect device type and serial number.
Detect Device	Click button to auto-detect device type and serial number. **Note:** Use of the auto-detect feature requires that the IP address and password of the device have been specified in the *IP-address* and *Root Password* fields.
Device Name	Name used to identify the device. To enable easy identification of devices, it is often a good idea to use a device name that refers to the physical area covered by the cameras attached to the device (examples: Reception Area, Car Park B, ...). **Note:** Device names must be unique; you cannot use the same name for several devices.

Field, Button, ...	Description
Camera Settings...	Opens the *Camera Settings for [Device Name]* window (see page 40), in which you are able to specify a number of settings for cameras attached to the device, including: • Port through which PTZ (Pan/Tilt/Zoom) cameras are controlled • Camera names, types, and ports **Note:** The number of settings available in the *Camera Settings for [Device Name]* window (see page 40) may be limited if cameras are not PTZ cameras or connected to a video encoder device.
Device Serial Number	Serial number of device; usually identical to the 12-character MAC address of the device (example: 0123456789AF). **Tip:** XProtect Enterprise is able to automatically detect serial number as well as device type, provided the IP address/host name and password of the device have been specified in the *IP-address/DNS Host Name* and *Root Password* fields: Simply click the *Detect Device* button to auto-detect device type and serial number.
Device License Key	A 16-character license key (DLK) for the device, obtained when registering the software.
Enable Fisheye	Enables the use of fisheye, a technology that allows viewing of 360-degree panoramic images. **Note:** Use of the fisheye technology requires either a dedicated fisheye camera or a regular camera equipped with a special fisheye camera lens for which a special fisheye license key is required. If the device in question is for a dedicated fisheye camera, the check box is selected by default, and you do not have to enter an fisheye license key in the neighboring field.
Fisheye License Key	License key for using the fisheye technology, obtained when registering the software. **Note:** This information is only required if the *Enable Fisheye* check box is selected manually.

Network Settings for Video Device Section

The Network Settings for Video Device section contains the following fields:

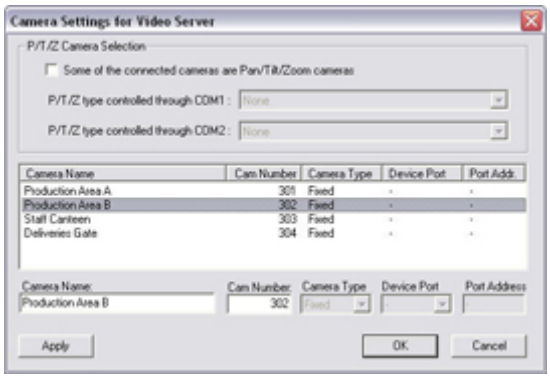
Field	Description
IP-address -or- **DNS Host Name**	IP address or DNS host name of the device in question. **Note:** If *Use DNS host name* check box is selected, the name of the *IP-address* field changes to *DNS/Host Name* in order to accommodate a DNS host name rather than an IP address.

Field	Description
Use DNS host name	By selecting the check box you are able to use a DNS host name for identifying the device instead of using the device's IP address. When check box is selected, the *IP-address* field changes its name to *DNS/Host Name*, ready to accommodate a DNS host name rather than an IP address.
Default Http Port	When selected, HTTP traffic to the device will go through the default port, port 80. If you want to use another port for HTTP traffic to the device, clear the check box, and specify required port number in the field to the left of the check box.
Default Ftp Port	When selected, FTP traffic to the device will go through the default port, port 21. If you want to use another port for FTP traffic to the device, clear the check box, and specify required port number in the field to the left of the check box.
Root Password	Password required in order to log in to the device using the root account (occasionally known as an *admin* or *administrator* account).

Camera Settings for [Device Name] Window

Note: The number of settings available in the *Camera Settings for [Device Name]* window may be limited if cameras are not PTZ (Pan/Tilt/Zoom) cameras or connected to a video encoder device.

The *Camera Settings for [Device Name]* window lets you specify certain information about a device's cameras. This is primarily interesting for PTZ cameras and cameras attached to a video encoder device. You access the *Camera Settings for [Device Name] window* by clicking the *Camera Settings...* button in the *Edit device settings* window (see page 38). The *Camera Settings for [Device Name]* window is divided into a *P/T/Z Camera Selection* section and a camera list:



P/T/Z Camera Selection Section

Field	Description
Some of the connected cameras are Pan/Tilt/Zoom cameras	Select check box if any of the cameras attached to the video encoder device is a PTZ camera. If the check box is not available, PTZ is not supported for the device in question.
P/T/Z type controlled through COM1	Field available only if *Some of the connected cameras are Pan/Tilt/Zoom cameras* check box is selected. If a PTZ camera is controlled through the COM1 port on the video encoder device, select the required PTZ camera

Field	Description
	type from the list. If no PTZ cameras are controlled through the COM1 port, select *None*.
P/T/Z type controlled through COM2	Field available only if *Some of the connected cameras are Pan/Tilt/Zoom cameras* check box is selected. If a PTZ camera is controlled through the COM2 port on the video encoder device, select the required PTZ camera type from the list. If no PTZ cameras are controlled through the COM2 port, select *None*.

Camera List and Fields

The camera list contains a line for each camera channel on the device. First line from the top corresponds to camera channel 1, second line from the top corresponds to camera channel 2, etc.

To change camera settings, select the required camera channel from the list, specify required information in the following fields, and click the *Apply* button:

Field	Description
Camera Name	Name used to identify the selected camera. Existing names, such as the default camera names *Camera 1, Camera 2*, etc. can be changed by overwriting the existing names. **Note:** Camera names must be unique for each device.
Cam Number	Users of the Smart Client can take advantage of a range of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers, which are used to identify each camera. Camera shortcut numbers must be unique for each camera, must not contain any letters or special characters, and must be no longer than eight digits. Examples of correct camera shortcut numbers: *3*, *12345678*. Examples of incorrect camera shortcut numbers: *A*3*, *123456789*. **Note:** Camera shortcut numbers are only used in the Smart Client. In other applications, such as the Remote Client, the camera shortcuts cannot be used. **Tip:** You can also assign shortcut numbers to cameras in the *Camera Name and Number* window (see page 64). **Tip:** More information about using the keyboard shortcuts is available in the separate Smart Client documentation.
Camera Type	Lets you select whether the camera on the selected camera channel is *Fixed* or *Moveable*: • *Fixed*: Camera mounted in a fixed position • *Moveable*: PTZ camera

Field	Description
Device Port	Available only if *Moveable* is selected in the *Camera Type* field. Lets you select which control port on the video encoder should be used for controlling PTZ functionality on the camera.
Port Address	Available only if *Moveable* is selected in the *Camera Type* field. Lets you specify port address of the camera. The port address would normally be *0* or *1*. If using daisy chained PTZ cameras, the port address will identify each of them, and you should verify your settings with those recommended in the cameras' manuals.

Using DVR Devices

You can easily use DVR (Digital Video Recorder) devices with XProtect Enterprise. You add DVR devices just like any other devices. In the *Administrator window* (see page 30), DVR devices will be listed in the same way as video encoders.

Access client users will experience no difference when viewing live video from a camera attached to at DVR compared to video from any other camera. However, when users view recordings from a DVR device, the recordings will be viewed from the hard disk of the DVR rather than from a camera database on the XProtect Enterprise server.

Note: The use of PTZ cameras is not supported for DVR devices.

Camera Administration

Adding and Configuring Cameras

In XProtect Enterprise you do not have to worry about having to add individual cameras to the system: Cameras are connected to devices, so once you have added the required devices to your XProtect Enterprise system (see How to Add a Device on page 36), all cameras connected to the devices are connected to the system as well.

You are able to specify a wide variety of settings for each camera connected to the XProtect Enterprise system. Your entry point for such camera configuration is the *Administrator* window (see page 30).

To configure a camera, select the required camera in the *Administrator* window's *Device Manager* section, then click the *Administrator* window's *Settings...* button. This will open the *Camera Settings for [Device Name] [Camera Name]* window (see below), in which you have access to settings for the camera in question, including:

- How the camera should record (frame rate, image quality, etc.)
- Where and when to store recorded video from the camera
- Motion detection sensitivity
- Triggering of notifications and external output
- ... and more

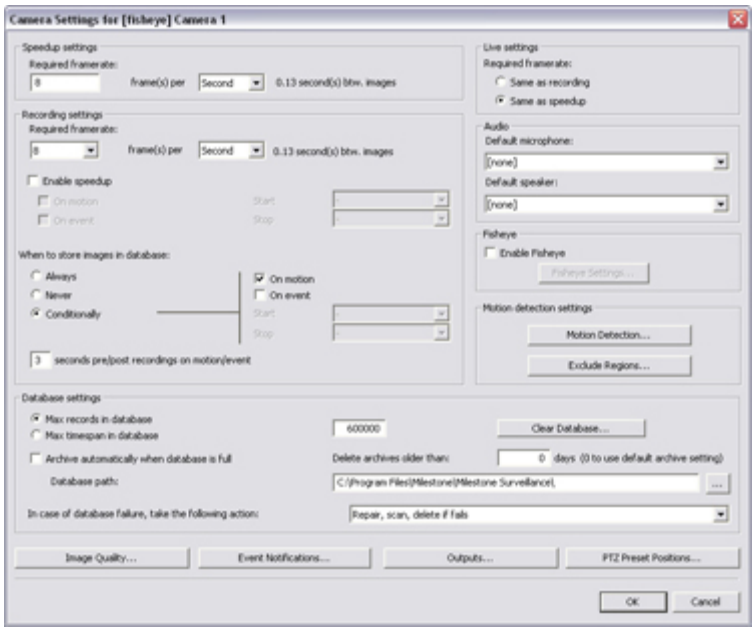
This also applies if you want to edit the settings for an already configured camera.

Camera Settings for [Device Name] [Camera Name] Window

The *Camera Settings for [Device Name] [Camera Name]* window lets you specify settings for a particular camera.

You access the *Camera Settings for [Device Name] [Camera Name]* window (see page 43) from the *Administrator* window (see page 30), by selecting a camera in the *Device Manager* section, then clicking the *Settings...* button.

The window contains the following sections and buttons:



Speedup Settings

The Speedup Settings section lets you specify the required number of frames to be used when motion is detected and/or an event occurs in this field.

- ***Required framerate*:** Specify required number of frames in the first field, and select required unit (per Second, per Minute, or per Hour) from the list. The frame rate must be higher than the frame rate specified in the *Required framerate* field in the *Recording settings* section which is described in the following.

Tip: When you specify a frame rate, the interval between images is automatically calculated and displayed to the right of the frame rate fields.

Specifically for cameras using MPEG: For MPEG cameras you can select predefined frame rates, and it is not possible to select unit. The number of seconds between each image is still calculated.

Recording Settings

The *Recording Settings* section lets you specify the camera's recording settings in the following fields:

- ***Required framerate*:** Specify required number of frames in the first field, and select required unit (per *Second*, per *Minute*, or per *Hour*) from the list. When you specify a frame rate, the interval between images is automatically calculated and displayed to the right of the frame rate fields.

  Specifically for Cameras Using MPEG: Instead of selecting required frame rate, you are able to select a *Frame Type*. Select *All* to record everything; that is similar to having the same frame rate for speedup and for recording. Select *Key frame* if you wish only to record key frames and ignore changes between the key frames; that means that you typically record one frame per second.

- **Enable speedup:** XProtect Enterprise is able to increase the frame rate of a camera if motion is detected, or if an event occurs. Select the check box to enable increased frame rate on motion detection or on an event, then specify the required conditions in the following fields.

  Tip: In the *Camera/Alert Scheduler* window (see page 71) you can specify periods in which the camera should *always* speedup.

  - *On motion*: Available only if the *Enable speedup* check box is selected. Select this check box to use a higher frame rate when motion is detected. Remember to specify the required higher frame rate in the *Speedup settings* section. The camera will return to the original frame rate two seconds after the last motion is detected.

  - *On event:* Available only if the *Enable speedup* check box is selected. Select the check box to use a higher frame rate when an event occurs and until another event occurs, then select required start and stop events in the *Start* and *Stop* lists. The camera will increase its frame rate when the start event occurs, and return to the original frame rate when the stop event occurs. Remember to specify the required higher frame rate in the *Speedup settings* section.

    Note: Use of speedup on event requires that at least one event (I/O, generic event, or VMD event) has been defined. Read more about events in About Input, Events & Output ... on page 84.

- ***When to store images in the database:*** Select when video received from the camera should be stored in the database:

- *Always*: Always store all received video in the database.
- *Never*: Never store any received video in the database. Live video will be displayed, but, since no video is kept in the database, users will not be able to browse video from the camera.
- *Conditionally*: Store received video in the database when certain conditions are met. When you select this option, specify required conditions in the following fields.

  On motion: Available only when the option *Conditionally* is selected, i.e. when video received from the camera should be stored in the database on certain conditions only. Select the check box to store all video in which motion is detected.

  On event: Available only when the option *Conditionally* is selected, i.e. when video received from the camera should be stored in the database on certain conditions only. Select the check box to store all video, regardless of motion, when an external event occurs and until another external event occurs, then select required start and stop events in the *Start* and *Stop* lists.

  Note: Use of storage on event requires that events have been defined. Read more about events in *About Input, Events & Output* ... on page 84

- [*Number of] seconds pre/post recordings on event:* Available only when the option *Conditionally* is selected, i.e. when video received from the camera should be stored in the database on certain conditions only.

  You are able to store recordings from periods preceding and following detected motion and/or specified events. Using such a *pre/post buffer* can be advantageous: If, for example, you have defined that video should be stored when a door is opened, being able to see what happened immediately prior to the door being opened may be important.

  Specify the numbers of seconds for which you want to store video from before and after the storage conditions are met. Example: You have specified that video should be stored conditionally on event, with a start event called *Door Opened* and a stop event called *Door Closed*. With a pre/post buffer of three seconds, video will be stored from three seconds *before Door Opened* occurs to three seconds *after Door Closed* occurs.

  Note: Pre/post recording periods cannot be displayed in the timelines of the *Smart Client*'s timeline browser. The fact that these periods cannot be displayed in the timeline browser's timelines does not affect recording.

Live Settings

The *Live settings* section lets you determine the frame rate with which users will view live video in their access clients. Select either *Same as recording* or *Same as speedup*.

Note: This section is not available for cameras using MPEG. For MPEG, viewing of live video will take place with the same frame rate as specified for speedup.

Audio

In the *Audio* section you are able to associate a microphone and/or speakers with the selected camera.

Note: The ability to associate a microphone and/or speakers with the selected camera requires that at least one microphone and/or speaker has been attached to a device on the surveillance system.

When a microphone and/or a speaker is associated with a camera, audio from the source will automatically be used when video from the camera is viewed. Note that you are able to select a microphone and/or speakers attached to another device than the selected camera.

To associate a microphone and/or speakers with the selected camera, simply select the required microphone and/or speakers from the *Default microphone* and *Default speaker* lists. For cameras attached to the same device as a microphone and/or speakers, the microphone and/or speaker is automatically selected and cannot be changed.

Fisheye

Note: Functionality in the *Fisheye* section is only available if the use of fisheye technology has been enabled for the device to which the camera is attached. For dedicated fisheye cameras, the use of fisheye technology is automatically enabled. If not dealing with a dedicated fisheye camera, you enable use of fisheye technology for a device in the *Edit device settings* window (see page 38), accessed by selecting the required device in the *Administrator* window's (see page 30) *Device Manager* section, then clicking the *Administrator* window's *Edit Device...* button.

The *Fisheye* section contains the following fields and buttons:

- **Enable Fisheye:** Select check box to enable the use of fisheye, a technology that allows viewing of 360-degree panoramic images through an advanced fish eye lens on the particular camera.

- **Fisheye Settings...**: Opens the *Fisheye Camera Configuration* window (see page 62), in which you configure the camera's fisheye functionality.

Motion Detection Settings

The *Motion Detection Settings* section contains two buttons for configuring the camera's motion detection:

- ***Motion Detection...:*** Opens the *Adjust Motion Detection* window (see page 50), in which you are able to specify motion detection sensitivity levels.

- ***Exclude Regions...:*** Opens the *Define Exclusion Regions* window (see page 52) where you are able to disable motion detection in specific areas of the camera's images.

  Disabling motion detection in certain areas may help you avoid detection of irrelevant motion, for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.

Database Settings

The database for each camera is capable of containing a maximum of 600,000 records or 40 GB per day. Note that camera databases also store recorded audio from associated audio sources; see Important Information about Using Audio page 66 for more information.

Tip: By using archiving (see page 125) it is possible to store recordings beyond the capabilities of the camera's database.

The *Database settings* section lets you specify database settings for the camera, such as where the database containing the camera's recordings should be kept, how much to store, etc. You specify this information in the following fields:

- ***Max records in database:*** Select this option to limit the database size based on a *maximum allowed number* of records in the database. Specify required maximum number of records in the neighboring field. When the database reaches the maximum number of records, the oldest record in the database will automatically be overwritten.

  Note: A database can contain a maximum of 600,000 records or 40 GB per day, regardless of what maximum has been defined.

- ***Max timespan in database*:** Select this option to limit the database size based on the *age* of records in the database. Specify the required number in neighboring field, and select required unit (*Minutes*, *Hours*, or *Days*) from the list. When records become older than the specified number of minutes, hours, or days, they will automatically be deleted.

  Note: A database can contain no more than 600,000 records or 40 GB per day, regardless of what maximum age has been defined.

  Tip: You will receive a message if—based on the recording frame rate you have specified for the camera—XProtect Enterprise detects that the maximum number of allowed records in the database is likely to be reached before the end of the specified time span.

- ***Clear Database... :*** Click button to delete all records stored in the database for the camera in question. Records stored in archived databases will not be affected.

  WARNING: Use with caution; all records in the database for the camera will be permanently deleted. As a security measure, you will be asked to confirm that you want to permanently delete all stored records for the camera.

  Note: If the *Milestone Recording Server* service is running, the button will not be available. To make the button available, pause the *Milestone Recording Server* service by clicking the *Administrator* window's (see page 30) *Service Manager* button, then clicking the *Pause* button or by stopping the service from the Recording Server Manager icon (see page 68).

  IMPORTANT: No video or audio will be recorded while the *Milestone Recording Server* service is paused or stopped (see page 68).

- ***Archive automatically when database is full:*** Select this check box if you wish to automatically archive the database when it is full.

  Note: For this feature to work, you should first enable archiving in the Archive Setup Window (see page 130).

- ***Delete archives older than [n] days (0 to use default archive setting):*** In this field you can specify after how many days archives for the camera should be deleted.

  Note: What you specify here overwrites what you have specified in the Archive Setup Window (see page 130). Type *0* to use same number of days as specified the Archive Setup window.

- ***Database path:*** Specify which local directory the database for the camera should be kept in. Default database path is the path at which the XProtect Enterprise software is installed, typically C:\Program Files\Milestone\Milestone Surveillance\. To browse for a folder, click the browse button next to the *Database path* field.

  Note: Even though it is possible to specify a path to a network drive, it is highly recommended that you specify a path to a *local* drive. If using a path to a network drive, it will not be possible to save to the database in cane the network drive should become unavailable.

Tip: If you have several cameras, and several local drives are available, performance can be improved by distributing the databases of individual cameras across the local drives.

- ***In case of database failure, take the following action:*** .Select which action to take if the database becomes corrupted. The number of available actions depends on whether archiving has been enabled. You enable archiving for a camera in the *Archive setup* window (see page 130), accessed from the *Administrator* window (see page 30) by clicking the *Archive Setup...* button.

    - *Repair, Scan, Delete if fails*: Default action. If the database becomes corrupted, two different repair methods will be attempted: a fast repair and a thorough repair. If both repair methods fail, the contents of the database will be deleted.

    - *Repair, Delete if fails*: If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be deleted.

    - *Repair, Archive if fails*: Available only if archiving is enabled for the camera. If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be archived. This action is recommended if archiving is enabled for the camera.

    - *Delete (no repair)*: If the database becomes corrupted, the contents of the database will be deleted.

    - *Archive (no repair)*: Available only if archiving is enabled for the camera. If the database becomes corrupted, the contents of the database will be archived.

      Tip: Provided the corrupted database has been archived (see page 125), it can be repaired by the *Viewer (*see page 169): Open the *Viewer* and attempt to browse the archived recordings from the camera in question. Browsing will initially fail, but this will make the *Viewer* start repairing the corrupt database.

  When the contents of the local database for the camera are either deleted or archived, the database is reset and will be ready for storing new recordings.

Note: Recording is not possible while the database is being repaired. For large installations, a repair may take several hours, especially if the *Repair, Scan, Delete if fails* action involving two different repair methods is selected, and the first repair method (fast repair) fails.

Tip: Learn how you can help prevent the need for repairing databases in the first place; see page 163.

Database Resizing

In case recordings for a camera get bigger than expected, or the available drive space is suddenly reduced in another way, an advanced database resizing procedure will automatically take place:

If archives are present on the same drive as the camera's database, the oldest archive for all cameras archived on that drive will be moved to another drive (moving archives is only possible if you use dynamic archiving, with which you can archive to several different drives; see page 134) or, if moving is not possible, deleted.

If no archives are present on the drive containing the camera's database, the size of all camera databases on the drive will be reduced by deleting a percentage of their oldest recordings, thus temporarily limiting the size of all databases

When the recording server is restarted upon such database resizing, the original database sizes will be used. You should therefore make sure the drive size problem is solved, or adjust camera database sizes to reflect the altered drive size.

Tip: Should the database resizing procedure take place, you will be informed on-screen in the Smart Client, in log files, and (if set up) through an e-mail and/or SMS alert.

Tip: For more information about how XProtect Enterprise responds to the threat of running out of disk space, see page 127.

Image Quality...

The *Image Quality...* button opens the *Configure Device* window (see page 50), in which you are able to configure resolution, compression, etc. for the camera.

Event Notification

The Event Notifications... button opens the Setup Notifications on Events window (see page 54), in which you are able to select events for triggering event indications for the camera when displayed in the Remote Client or Smart Client (see page 175).

Note: The use of event notifications requires that at least one event has been specified for a device on your XProtect Enterprise system; the event does not have to be specified for the particular camera. Read more about events in *About Input, Events & Output* .... on page 84

Outputs...

The *Outputs...* button opens the *Output Settings for [Device Name] [Camera Name]* window (see page 53), in which you are able to specify which outputs (e.g. the sounding of a siren or the switching on of the lights) should be associated with motion detection and/or with output buttons for manually triggering output when the camera is selected in the Remote Client or Smart Client (see page 175).

Note: The use of outputs requires that at least one event has been specified for a device on your XProtect Enterprise system; the event does not have to be specified for the particular camera. You specify output events in the *I/O Setup* window (see page 86), accessed by clicking the *I/O Setup...* button in the *Administrator* window (see page 30).

PTZ Present Position... (PTZ Cameras Only)

Available only if the camera is a PTZ (Pan/Tilt/Zoom) camera supporting PTZ preset positions, the PTZ Preset Positions... button opens *PTZ Preset Positions for [Device Name] [Camera Name]* window (see page 56), in which you are able to specify preset positions and patrolling for the camera.

Note: If the Milestone Recording Server service (see page 68) is running, the button will not be available. To make the button available, pause the Milestone Recording Server service by clicking the Administrator window's (see page 30) Service Manager... button, then clicking the Pause button.

IMPORTANT: No video or audio will be recorded while the *Milestone Recording Server* service is paused.

Configure Device Window

Note: Settings in the *Configure Device* window are to a large extent camera-specific. The window's contents will therefore vary from camera to camera; descriptions in the following are thus for guidance only.

The *Configure Device* window lets you specify image quality settings, such as compression, resolution, etc. for a specific camera. You access the *Configure Device* window by clicking the *Image Quality...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 43). The *Configure Device* window is divided into a *Camera Settings* section and a section with a preview image.

Camera Settings Section

The *Camera Settings* section will typically contain controls for compression, bandwidth, resolution, color, contrast, brightness, rotation, and similar.

Include Date and Time in Image

The *Camera Settings* section may feature an *Include Date and Time in Image* check box. When selected, date and time *from the camera* will be included in images from the camera.

Note: As cameras are separate units which may have separate timing devices, power supplies, etc., camera time and XProtect Enterprise system time may not correspond fully, and this may occasionally lead to confusion. As all images are time-stamped by XProtect Enterprise upon reception and exact date and time information for each image is thus already known, it is recommended that you keep the *Include Date and Time in Image* check box cleared. Should you want to use the *Include Date and Time in Image* feature, it is recommended that you click the *Synchronize Time* button, if available. Clicking the *Synchronize Time* button will set camera time to system time, but does not guarantee that camera time will match system time indefinitely.

Tip: For consistent synchronization, you may, if supported by the camera, auto-synchronize camera and system time via a time server.

Preview Image

When adjusting camera settings, you are able to view the effect of your settings by clicking the *Preview Image* button, located at the bottom of the window. Clicking the *Preview Image* button will provide you with an image from the camera in question, as it would look with the settings specified in the *Camera Settings* section. When you have found the best possible camera settings, click *OK* to apply the settings for the camera.

Adjust Motion Detection Window

The *Adjust Motion Detection* window lets you specify motion detection sensitivity for a specific camera. Depending on your configuration, motion detection sensitivity settings may determine when recordings from the camera are transferred to the surveillance system, when alerts are generated, when external outputs (such as lights or sirens) are triggered, etc.

Motion detection sensitivity is therefore a key element in your XProtect

Enterprise surveillance solution, and time spent on finding the best possible motion detection settings for each camera may help you later avoid unnecessary alerts, etc.

Depending on the physical location of the camera, it may be a very good idea to test motion detection settings under different physical conditions (day/night, windy/calm weather, etc.).

You access the *Adjust Motion Detection* window by clicking the *Motion Detection...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 43).

Note: Before you configure motion detection sensitivity for a camera, it is highly recommended that you have configured the camera's image quality settings, such as resolution, compression, etc., in the *Configure Device* window (see page 50), and that you have specified any areas to be excluded from motion detection (for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background) in the *Define Exclusion Regions* window (see page 52). If you later change image quality settings and/or exclusion area settings, you should always test motion detection sensitivity settings afterwards.

The *Adjust Motion Detection* window features two sliders; one for setting *Noise Sensitivity* and one for setting *Motion Sensitivity*:

Noise Sensitivity

Noise is insignificant changes in individual pixels which should not be regarded as motion.

The *Noise Sensitivity* slider determines how much each pixel must change before it is regarded as motion. Insignificant changes, which should not be regarded as motion, are considered acceptable noise, hence the name of the slider. With high noise sensitivity, very little change in a pixel is required before it is regarded as motion.

Tip: If you find the concept of noise sensitivity difficult to grasp, try dragging the slider to the left towards the *High* position: The more you drag the slider towards the *High* position, the more of the preview image becomes highlighted. This is because with high noise sensitivity even the slightest change in a pixel will be regarded as motion.

Areas in which motion is detected are highlighted in the preview image. Select a slider position in which only detections you consider motion are highlighted.

As an alternative to using the slider, you may specify a value between 0 and 256 in the field next to the slider to control the noise sensitivity setting.

Motion Sensitivity

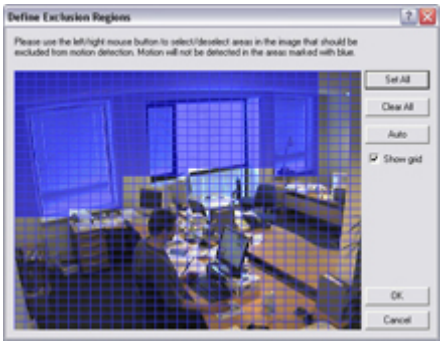
The *Motion Sensitivity* slider determines how many pixels must change in the image before it is regarded as motion.

The selected motion sensitivity level is indicated by the black vertical line in the motion level indication bar below the preview image. The black vertical line serves as a threshold: When detected motion is above the selected sensitivity level, the bar changes color from green to red, indicating a positive detection.

As an alternative to using the slider, you may specify a value between 0 and 10,000 in the field next to the slider to control the motion sensitivity setting.

Define Exclusion Regions Window

The *Define Exclusion Regions* window lets you disable motion detection in specific areas of a camera's images. Disabling motion detection in certain areas may help you avoid detection of irrelevant motion, for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.


Define Exclusion Regions
Please use the left/right mouse button to select/deselect areas in the image that should be excluded from motion detection. Motion will not be detected in the areas marked with blue.
Set All
Clear All
Auto
Show grid
OK
Cancel
The Define Exclusion Regions window, with an exclusion area highlighted in blue

You access the *Define Exclusion Regions* window by clicking the *Exclude Regions...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 43).

Defining Areas in which Motion Detection Should Be Disabled

The *Define Exclusion Regions* window features a preview image from the camera. You define the areas in which motion detection should be disabled in the preview image, which is divided into small sections by a grid.

To define areas in which motion detection should be disabled, drag the mouse pointer over the required areas in the preview image while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in blue.

Define Exclusion Regions Window's Buttons and Check Boxes

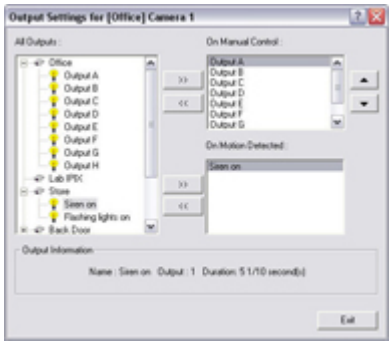
The *Define Exclusion Regions* window features the following buttons:

Button, Check Box	Description
Set All	Lets you quickly select all grid sections in the preview image. This may be advantageous if you want to disable motion detection in most areas of the image, in which case you can simply clear the few sections in which you do not want to disable motion detection.
Clear All	Lets you quickly clear all grid sections in the preview image.
Auto	By clicking the *Auto* button you can make XProtect Enterprise automatically detect areas with noise (insignificant changes in individual pixels which should

Button, Check Box	Description
	not be regarded as motion) in the image, and automatically mark such areas as areas in which motion detection should be disabled. As the automatic detection is based on an analysis of a number of images, it may take a few seconds from you click the *Auto* button to noisy areas are detected and marked as areas in which motion detection should be disabled. **Note:** The automatic detection of noisy areas happens according to the noise sensitivity setting specified in the *Adjust Motion Detection* window (see page 50). In order for the automatic detection of noisy areas to work as intended, it is recommended that you specify a noise sensitivity setting that matches your requirements before you make use of the automatic detection feature.
Show Grid	With the *Show grid* check box selected (default), the preview image contains a grid indicating the division of the preview image into selectable sections. With the *Show grid* check box cleared, the grid in the preview image is removed. This may provide a less obscured view of the preview image. Selection of areas in which motion detection should be disabled takes place the same way as when the grid is visible.

Output Settings for [Device Name] [Camera Name] Window

In the *Output Settings for [Device Name] [Camera Name]* window you are able to associate a camera with particular external outputs, defined in the *I/O Setup* window (see page 86), for example the sounding of a siren or the switching on of lights.



The associated outputs can be triggered automatically when motion is detected as well as manually through output buttons available in the Remote Client and Smart Client (see page 175).

You access the *Output Settings for [Device Name] [Camera Name]* window from the *Camera Settings for [Device Name] [Camera Name]* window (see page 43), by clicking the *Outputs...* button.

Associating Outputs with Manual Control and Detected Motion

Note: Use of features in the *Output Settings for [Device Name] [Camera Name]* window requires that output has been defined in the *I/O Setup* window (see page 86).

You have a high degree of flexibility when associating a camera with particular outputs:

- You are able to select between all available outputs, i.e. outputs defined as output events for the camera itself **as well as** outputs defined as output events for other devices on the XProtect Enterprise system
- The same output may be used for manual control through an output button **as well as** for automatic triggering when motion is detected

Selecting Output for Manual Control

You are able to specify outputs to be triggered manually from a list in the Remote Client or Smart Client (see page 175).

To specify an output for manual triggering in the Remote Client/Smart Client, do the following:

1. Select the required output in the *All Outputs* list in the left side of the *Output Settings for [Device Name] [Camera Name]* window.

   Tip: When you select an output in the *All Outputs* list, you can view detailed information about the selected output under *Output Information* in the lower part of the window.

2. Click the >> button located between the *All Outputs* list and the *On Manual Control* list. This will copy the selected output to the *On Manual Control* list.

An unlimited number of outputs may be selected this way.

You are able to determine each output's position in the Remote Client's and Smart Client's output list by moving the selected output up or down in the *On Manual Control* list with the *up* and *down* buttons located to the right of the list. The selected output is moved up one step each time you click the *up* button. Likewise, each time you click the *down* button, the selected output is moved down one step.

To remove an output from the *On Manual Control* list, simply select the required output, and click the << button located between the *All Outputs* list and the *On Manual Control* list.

Selecting Output for Use on Motion Detection

You are able to select outputs to be triggered automatically when motion is detected in video from the camera.

Tip: This feature does not require that a VMD (Video Motion Detection) event has been defined for the camera in the *I/O Setup* window (see page 86).

To select an output for use when motion is detected in video from the camera:

1. Select the required output in the *All Outputs* list in the left side of the *Output Settings for [Device Name] [Camera Name]* window.

   Tip: When you select an output in the *All Outputs* list, you can view detailed information about the selected output under *Output Information* in the lower part of the window.

2. Click the >> button located between the *All Outputs* list and the *On Motion Detected* list.

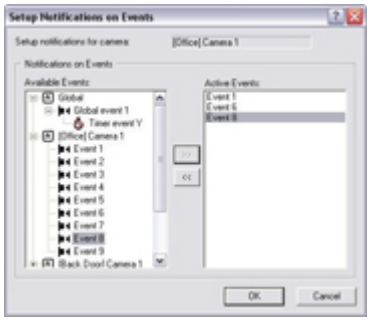
   This will copy the selected output to the *On Motion Detected* list.

To remove an output from the *On Motion Detected* list, simply select the required output, and click the << button located between the *All Outputs* list and the *On Motion Detected* list.

Setup Notifications on Events Window

Note: The use of event notifications requires that at least one event has been specified for a device on your XProtect Enterprise system; the event does not have to be specified for the particular

camera. You specify events in the *I/O Setup* window (see page 86), accessed by clicking the *I/O Setup...* button in the *Administrator* window (see page 30).

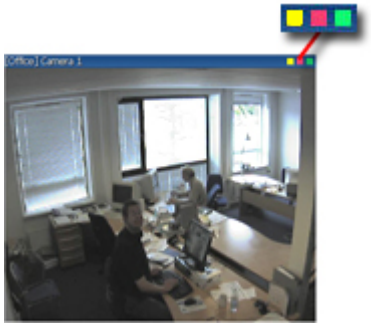


The *Setup Notifications on Events* window lets you select events for triggering event indications for the camera when displayed in *Remote Client* and *Smart Client* (see page 175).

You access the *Setup Notifications on Events* window from the *Camera settings for [Device Name] [Camera Name]* window (see page 43), by clicking the *Event Notifications* button.

What is an Event Indication?

In the *Remote Client*/*Smart Client*, three different color indicators are available for each camera: a yellow indicator, a red indicator, and a green indicator. When event indication is used for a camera, the yellow indicator will light up when the specified events have occurred.



Event indications can be valuable for camera operators, as they will be able to quickly detect that an event has occurred, even though their focus was perhaps on something else the moment the event occurred.

Tip: The other two indicators serve the following purposes: The red indicator lights up when motion has been detected, and the green indicator is used for indicating that video is received from a camera.

Specifying Events for which Event Indication Should Be Used

To specify which events should trigger an event indication for the camera, do the following for each required event:

1. In the *Available Events* list, select the required event.

   Tip: You are not limited to events associated with a particular device: You are able to select between all available events (input events, timer events, event buttons) from all cameras on the XProtect Enterprise surveillance system.

2. Click the >> button to copy the selected event to the *Active Events* list. When an event listed in the *Active Events* list occurs, the event indicator will light up.

3. Repeat for each required event.

To remove an event from the *Active Events* list, select the event in question, and click the << button.

PTZ Preset Positions for [Device Name] [Camera Name] Window

Available only when dealing with a PTZ (Pan/Tilt/Zoom) camera supporting PTZ preset positions, the *PTZ Preset Positions for [Device Name] [Camera Name]* window lets you view and — for many, but not all, PTZ cameras — define preset positions for the PTZ camera.

To access the *PTZ Preset Positions for [Device Name] [Camera Name]* window, click the *PTZ Preset Positions...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 43). The button is only available if the camera supports PTZ preset positions. Note that if the *Milestone Recording Server* service (see page 68) is running, the button will not be available; see the description of the *Camera Settings for [Device Name [Camera Name]* window for information about how to make the button available.

Why Use Preset Positions?

Defined preset positions can be used for making the PTZ camera automatically go to particular preset positions when particular events occur, and for specifying PTZ patrolling schemes. Defined preset positions will also become selectable in the *Remote Client*/*Smart Client*, allowing users of these applications to move the PTZ camera to the preset positions.

Absolute and Relative Positioning PTZ Cameras

Your configuration options depend on whether the PTZ camera in question is of the absolute positioning or relative positioning kind:

- ***Absolute*:** For an absolute positioning PTZ camera, you are able to define up to 50 preset positions. You define a preset position by moving the PTZ camera to the required position with the controls in the *PTZ View* section, then naming the position in the window's *Preset Positions* section.

- ***Relative*:** For a relative positioning PTZ camera, the number of preset positions will depend on the camera/video encoder and PTZ driver used. For some relative positioning PTZ cameras you will only be able to use preset positions defined on the camera/video encoder itself (when this is the case, the preset positions are typically defined through the camera/video server's "built-in" web page).

  For relative positioning PTZ cameras allowing definition of preset positions through the XProtect Enterprise system, you define a preset position by moving the PTZ camera to the required position with the controls in the *PTZ View* section, then naming the position in the window's *Preset Positions* section.

How to Define a Preset Position

Note: Some PTZ cameras of the relative positioning kind do not allow you to define preset positions as described in the following; for such cameras, you should define preset positions on the camera/video encoder itself.

1. First use the controls in the *PTZ Preset Positions for [Device Name] [Camera Name]* window's *PTZ View* section to move the PTZ camera to the required position.

2. Having moved the PTZ camera to the required position, select an undefined item (may be labeled *Undefined* or with a position number) in the *Preset Positions* section's list of preset position names, and click the *Set Position* button to define a name for the preset position.

   For detailed information about the functionality of *PTZ Preset Positions for [Device Name] [Camera Name]* window—such as the ability to test your preset positions, the ability to combine preset positions with events, or the ability to use preset positions in PTZ patrolling schemes—see *Preset Positions for [Device Name] [Camera Name]* window's sections in the following.

You are able to define up to 50 preset positions.

Each of the *PTZ Preset Positions for [Device Name] [Camera Name]* window's sections are described in the following:

PTZ View Section

The *PTZ View* section lets you control the PTZ camera, and watch the PTZ camera's movements. You use this section to move the PTZ camera to the positions you then define as presets positions in the *Preset Positions* section.

To move the PTZ camera, simply click the required position in the preview picture.

The *PTZ View* section also features sliders allowing you to move the PTZ camera along each of its axes: the X-axis (allowing you to pan left/right), the Y-axis (allowing you to tilt the camera up/down), and the Z-axis (enabling you to zoom in and out; the camera will zoom in when you move the slider towards *Tele*, and zoom out when you move the slider towards *Wide*).

As an alternative to clicking the required position in the preview or using the sliders, you can use the PTZ camera navigation buttons:

Moves the PTZ camera up and to the left

Moves the PTZ camera up

Moves the PTZ camera up and to the right

Moves the PTZ camera to the left

Moves the PTZ camera to its home position

Moves the PTZ camera to the right

Moves the PTZ camera down and to the left

Moves the PTZ camera down

Moves the PTZ camera down and to the right

Zoom out (one zoom level per click)

Zoom in (one zoom level per click)

Preset Position Section

Having specified a camera position in the *PTZ View* section, you define the required position as a preset in the *Preset Positions* section:

Button, Check Box	Description
Use preset positions from device	Available only for cameras supporting this feature. Check box to use preset positions defined on the camera or video encoder device. Using preset positions from the camera or video encoder device will clear any preset positions you have defined for the PTZ camera; you will therefore be asked to confirm your selection. **Note:** In order for preset positions from the camera or video encoder device to work with XProtect Enterprise, the names of the preset positions must contain only the characters A-Z, a-z and 0-9, and must not contain spaces. If preset position names on the camera or video encoder device contain other characters, or spaces, change the preset position names on the device before selecting the *Use preset positions from device* feature.
Set Position	Associates the preset position selected in the list with the position specified in the *PTZ View* section. If the preset position selected in the list is yet undefined, you will be asked to specify a name for the preset position.
Edit Name...	Lets you edit a preset position name selected in the list. Only works for an already defined preset position name.
Test	Lets you test a defined preset position. Select the required preset position in the list, then click the *Test* button. The effect is displayed instantly in the *PTZ View* section.
Delete	Lets you delete a preset position selected in the list. When a preset position name is deleted, it will appear as undefined in the list.
[Move up] **[Move down]**	Lets you move a preset position selected in the list up and down respectively. The selected preset position is moved one step per click. By moving preset position up or down, you are able to control the sequence in which available preset positions are presented in the *Remote Client* and *Smart Client* (see page 175). In the *Remote Client* and *Smart Client*, users select preset positions from a list. By moving a preset position up or down in the *Preset Positions* section's list, you can thus determine the sequence in which preset positions are presented in the *Remote Client*'s or *Smart Client*'s list. Display of preset positions in Remote Client/Smart Client. Administrators are able to specify the sequence in which available preset positions are displayed.

Preset Position on Event Section

If you have specified input or VMD events (see page 86), event buttons (see page 96) or generic events (see page 100), you are able to make the PTZ camera automatically go to particular preset positions when particular events occur.

To configure the use of preset positions on events, click the *Setup...* button. This will open the *Event* window (for preset positions on event) – see page 59) – in which you are able to associate particular preset positions with particular events.

To use preset positions on event, select the *Go to preset on event* check box.

Patrolling Section

To configure PTZ patrolling (the automatic movement of a PTZ camera between several preset positions), click the *Setup...* button to go to the *Setup PTZ Patrolling* window (see page 60).

PTZ patrolling requires that at least two preset positions have been defined.

Event Window (for PTZ Preset Positions on Events)

Available only when dealing with a PTZ (Pan/Tilt/Zoom) camera, the *Event* window (for preset positions on events) lets you associate particular preset positions with particular events, timer events or event buttons. You are thus able to make the PTZ camera automatically go to a particular preset position when a particular event occurs.

To access the *Event* window (for preset positions on events), click the *Setup...* button in *Preset Position on Events* section of the *PTZ Preset Positions for [Device Name] [Camera Name]* window (see page 56).

Note: To use preset positions on events, you must have specified input or VMD events (see page 86), event buttons (see page 96) or generic events (see page 100). Only one PTZ preset position can be defined per event per camera.

Associating Preset Positions with Particular Events

When associating a preset position from a particular PTZ camera with one or more events, you are able to select between **all** events defined on the XProtect Enterprise system; you are not limited to selecting events defined on a particular device.

To associate a particular preset position with a particular event, do the following:

1. Select the required preset position in the *Available Preset Positions* list in the left side of the *Event* window.

2. Select the required event in the list of available events (the list in the middle of the window).

3. Click the >> button located to the right of the *Available Events* list.

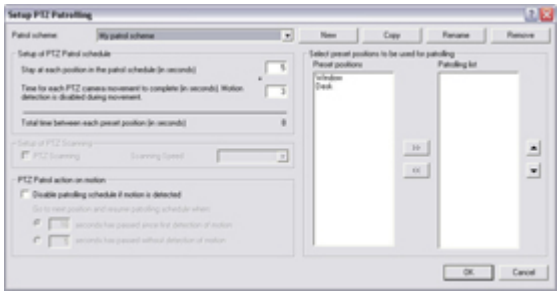
This will copy the selected event to the window's rightmost list, in which events associated with the selected preset position are listed. When the selected event occurs, or when the selected event button is clicked, the PTZ camera will automatically move to the required preset position.

You are able to associate a preset position with more than one event: Simply repeat the process for each required association.

To end the association between a particular preset position and a particular event, simply select the required event in the window's rightmost list, and click the << button.

Setup PTZ Patrolling Window

Available only when dealing with a PTZ (Pan/Tilt/Zoom) camera, the *Setup PTZ Patrolling* window lets you configure patrol schemes for PTZ patrolling (the automatic movement of a PTZ camera between several preset positions) for the camera.



To access the *Setup PTZ Patrolling* window, click the *Setup...* button in *Patrolling* section of the *PTZ Preset Positions for [Device Name] [Camera Name]* window (see page 56).

Note: To use patrolling, you must have specified at least two preset positions for the PTZ camera in question.

Tip: Although it is technically not patrolling, specifying a patrol scheme with only one preset position is possible. A patrol scheme with only one preset position can, when combined with scheduling (see page 71), be useful in two cases: For moving a PTZ camera to a specific position at a specific time, and for moving a PTZ camera to a specific position upon manual PTZ control of the camera.

Note: When you have defined your patrol schemes, also remember to schedule use of the patrol schemes in the *Camera/Alert Scheduler* window (see page 71).

Note: Bear in mind that patrolling can be overridden if operators (with the necessary user rights) manually control PTZ cameras.

Patrol Scheme

A PTZ camera may patrol according to several different patrol schemes. For example, a PTZ camera in a supermarket may patrol according to one patrol scheme during opening hours and according to another patrol scheme when the supermarket is closed.

The *Patrol scheme* list lets you select which patrol scheme to configure.

Defining a New Patrol Scheme

To define a new patrol scheme, click the *New* button. This will add a *New patrol scheme* listing to the *Patrol scheme* list.

To change the name from *New patrol scheme* to a name of your choice, select the *New patrol scheme* listing, and click the *Rename* button.

Copying an Existing Patrol Scheme

If you want to create a new patrol scheme based on an existing one, you can copy the existing patrol scheme.

To copy an existing patrol scheme, select the required patrol scheme in the *Patrol scheme* list, and click the *Copy* button. This will add a copy of the selected patrol scheme to the list.

The copy will initially be named *Copy of [Patrol Scheme Name]*. To change the name to a name of your choice, select the *Copy of [Patrol Scheme Name]* listing, and click the *Rename* button.

Renaming an Existing Patrol Scheme

To change the name of an existing patrol scheme, select the required patrol scheme in the *Patrol scheme* list, and click the *Rename* button.

Removing an Existing Patrol Scheme

To remove an existing patrol scheme, select the required patrol scheme in the *Patrol scheme* list, and click the *Remove* button.

Note: The selected patrol scheme will be removed from the list without further warning.

Selecting Preset Positions to Be Used for a PTZ Patrol Scheme

Having selected a patrolling scheme in the *Patrol scheme* list, you are able to specify which of the PTZ camera's preset positions should be used for the selected patrolling scheme:

1. In the *Preset Positions* list, select the names of the preset positions you want to use.

   A preset position can be used more than once in a patrol scheme, for example if the preset position covers an especially important location.

   Tip: By pressing the CTRL or SHIFT buttons on your keyboard while selecting from the *Preset Positions* list, you are able to select several or all of list's preset positions in one go.

2. Click the >> button to copy the selected preset positions to the *Patrolling list*.

3. The camera will move between preset positions in the sequence they appear in the *Patrolling list*, starting at the preset position listed first.

   If you want to change the sequence of preset positions in the *Preset Positions* list, select a preset position name, and use the *move up* or *move down* buttons to move the selected preset position name.

To remove a preset position from the *Patrolling list*, select the preset position in question, and click the << button.

Specifying Timing Settings for a PTZ Patrol Scheme

Having selected a patrolling scheme in the *Patrol scheme* list, you are able to specify timing settings for the patrol scheme:

1. In the *Stay at each position in the patrol schedule* field, specify the number of seconds for which the PTZ camera should stay at each preset position.

2. In the *Time for each PTZ camera movement to complete* field, specify the number of seconds required for the PTZ camera to move between preset positions.

   In order not to generate false motion alarms, motion detection for the PTZ camera is automatically disabled while the camera moves between two preset positions. After the specified number of seconds, motion detection is automatically enabled again. It is thus important that the camera is able to reach all of the patrolling scheme's preset positions within the number of seconds you specify. If not, false motion is likely to be detected.

   Bear in mind that it takes longer for the PTZ camera to move between positions that are located physically far apart (e.g. from an extreme left position to an extreme right position) than between positions that are located physically close together.

3. The total number of seconds between each preset position will be listed below the two fields.

PTZ Patrolling Actions on Detected Motion

You are able to combine a PTZ patrol scheme with motion detection, so that when motion is detected, the PTZ camera will pause its patrolling and remain at the position where motion was detected for a specified period of time:

1. Select the *Disable patrolling schedule if motion is detected* check box.

2. Select whether the PTZ camera should resume patrolling:

   - When a certain number of seconds has passed since first detection of motion, regardless whether further motion is detected

     - or -

   - When a certain number of seconds has passed without further detection of motion

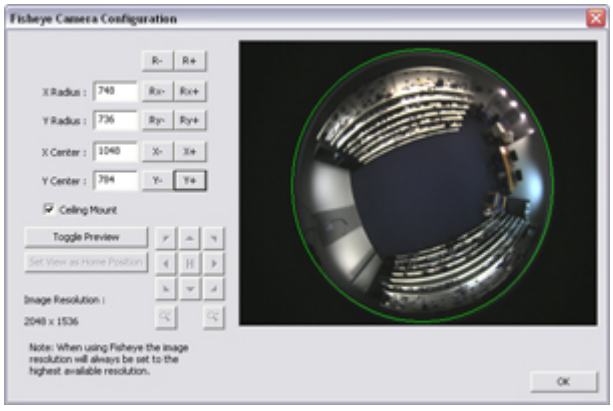
3. Specify the required number of seconds for selected option.

   Example: You may specify that the PTZ camera should go to the next preset position and resume patrolling when 10 seconds has passed without detection of motion.

PTZ Scanning

PTZ scanning is supported on a few devices only. If your device supports PTZ scanning, the *Setup of PTZ Scanning* section lets you enable PTZ scanning and select a PTZ scanning speed.

Fisheye Camera Configuration Window



Note: Use of the fisheye technology requires a dedicated fisheye camera or a special fisheye camera lens with a special fisheye license key, specified in the *Edit Device Settings* window (see page 38).

Fisheye is a technology that allows viewing of 360-degree panoramic images through an

advanced fisheye lens. The *Fisheye Camera Configuration* window lets you configure the fisheye functionality of a camera.

You access the *Fisheye Camera Configuration* window from the *Camera Settings for [Device Name] [Camera name]* window (see page 43), by selecting the *Enable Fisheye* check box, and clicking the *Fisheye Settings...* button.

Fisheye View Adjustment

The camera's fisheye functionality is configured by adjusting its fisheye view field—indicated by a green ellipse in the preview image—so it encloses the actual image area of the "fish eye" lens. You do this by specifying a number of values which will be used by the fisheye technology for converting the elliptic image into an ordinary rectangular image.

You are able to set the ellipse's X-radius, Y-radius, X-center, and Y-center, either by specifying the required values directly in the four fields or by using the following buttons to adjust the ellipse:

Button	Description
R-	Decreases the radius of the fisheye view field. The ellipse's horizontal (X) and vertical (Y) radiuses are changed at the same time, keeping the aspect ratio.
R+	Increases the radius of the fisheye view field. The ellipse's horizontal (X) and vertical (Y) radiuses are changed at the same time, keeping the aspect ratio.
Rx-	Decreases the horizontal (X) radius of the ellipse.
Rx+	Increases the horizontal (X) radius of the ellipse.
Ry-	Decreases the vertical (Y) radius of the ellipse.
Ry+	Increases the vertical (Y) radius of the ellipse.
X-	Moves the ellipse to the left.
X+	Moves the ellipse to the right.
Y-	Moves the ellipse up.
Y+	Moves the ellipse down.

Previewing the Fisheye View

You are able to toggle between previewing the original elliptic view as well as the "flattened" rectangular view resulting from applying the fisheye algorithm according to your specified values. To toggle between the two different types of preview, click the *Toggle Preview* button.

When previewing the fisheye-rendered view, the following navigation buttons become available for moving around within the preview image area:

	Moves the fisheye-rendered view up and to the left
	Moves the fisheye-rendered view up
	Moves the fisheye-rendered view up and to the right
	Moves the fisheye-rendered view to the left
	Moves the fisheye-rendered view to its home position
	Moves the fisheye-rendered view to the right
	Moves the fisheye-rendered view down and to the left
	Moves the fisheye-rendered view down
	Moves the fisheye-rendered view down and to the right
	Zoom out (one zoom level per click)
	Zoom in (one zoom level per click)

Ceiling Mounted Cameras

If the camera is mounted on a ceiling, you can adjust the behavior of the navigation buttons to reflect this by selecting the *Ceiling Mount* check box.

Setting a View as Home Position

When previewing the fisheye-rendered view, you are able to set a particular position in the fisheye-rendered view as the camera's PTZ home position: Navigate to the required position, using the navigation buttons and then click the *Set View as Home Position* button.

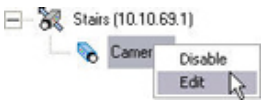
Image Resolution

Resolution values are automatically displayed in the lower part of the window, next to the navigation buttons. When using fisheye, resolution will automatically be set to the highest available resolution.

Camera Name and Number Window

The *Camera Name and Number* window lets you edit the name of a selected camera, and, if required, assign a shortcut number to the selected camera.

You access the *Camera Name and Number* window from the *Administrator* window's (see page 30) *device Manager* section: Right-click the name of the required camera, then select *Edit* from the menu that appears:



The *Camera Name and Number* window contains two fields:

Field	Description
Camera Name	Displays the name of the camera. If required, you are able to overwrite the existing camera name with a new one.
Camera Number	Users of the *Smart Client* (see page 175) can take advantage of a range of keyboard shortcuts, some of which let the users toggle between viewing different cameras. Such shortcuts include numbers, which are used to identify each camera. Camera shortcut numbers must be unique for each camera, must not contain any letters or special characters, and must be no longer than eight digits. Examples of correct camera shortcut numbers: *3*, *12345678*. Examples of incorrect camera shortcut numbers: *A*3*, *123456789*. **Note:** Camera shortcut numbers are only used in the *Smart Client* (see page 175). In other applications, such as the *Remote Client*, the camera shortcuts cannot be used. **Tip:** More information about using the keyboard shortcuts is available in the documentation for the Smart Client.

Audio Source Administration

Important Information about Using Audio

If you use audio sources (i.e. microphones and/or speakers) on your XProtect Enterprise system, note the following:

- **Only audio from microphones is recorded:** Only incoming audio, i.e. audio recorded by microphones attached to cameras, is recorded. Outgoing audio, i.e. what Smart Client operators say when they talk through speakers attached to cameras, is not recorded.

- **Audio from microphones is recorded even when video is not:** When a microphone is enabled (see Microphone Settings Window described on page 67), audio from the microphone will be recorded whenever the associated camera is online (i.e. transmitting data to XProtect Enterprise; see Camera/Alert Scheduler Window on page 71), regardless whether video from the camera is being recorded or not.

  Depending on your cameras' recording settings, this may mean that when you play back recordings, you may find that there are periods for which you only have audio recordings. This will also be the case for exported recordings if audio has been included in the export.

- **Audio recording affects video storage capacity:** When a microphone is enabled, audio is recorded to the associated camera's database. This will affect the database's capacity for storing video. A camera's database can contain a maximum of 40 GB or 600,000 records. It is thus important to bear in mind that the maximum limit of the database is likely to be reached earlier if recording audio *and* video than if only recording video.

  - Example: If using MPEG4, each one-second video GOP (Group Of Pictures) will be stored in one record in the database. Each second of audio will also be stored in one record in the database. When this is the case, the database's video storage capacity will be reduced to a maximum of 300,000 records, because half of the database's total maximum of 600,000 records will be used for storing audio.

  - Example: If using MJPEG, audio is stored in one record for every JPEG for as long as the audio block size does not exceed the time between the JPEGs. The database's video storage capacity can thus in extreme cases be reduced to a maximum of 300,000 records, because half of the database's total maximum of 600,000 records will be used for storing audio. If using very high frame rates, where there is less time between each JPEG, a smaller portion of the database will be used for storing audio records, and consequently a larger portion will be available for storing video.

  Thus, a camera database's maximum video storage capacity may in some cases be halved when an associated audio source is enabled.

  Note: Above examples are simplified. Since databases also have a maximum limit of 40 GB of data, the exact available video storage capacity will also depend on GOP/JPEG and audio kilobyte size.

  Tip: The Archiving feature (see page 125) enables you to store recordings beyond the capabilities of cameras' databases. Even if already using archiving, you may want to archive more frequently if recording audio and video than if only recording video.

Microphone Settings Window

The *Microphone Settings* window lets you change basic settings for a microphone.

You access the *Microphone Settings* window from the Administrator window (see page 30): Select a microphone in the *Administrator* window's *Device Manager* section, then click the *Settings* button.

- ***Device name:*** Displays the name of the microphone. If required, you are able to overwrite the existing audio microphone name with a new one.

- ***Enabled:*** Lets you enable/disable use of the microphone.

Tip: You can also enable/disable an audio source in the *Administrator* window: Right-click the required audio source in the *Administrator* window's *Device Manager* section, then select *Disable* or *Enable* from the menu that appears.

Note: On some devices, a microphone can also be enabled/disabled on the device itself, typically through the device's own configuration web page. If a microphone on a device does not work after enabling it in the *Administrator* application, you should thus verify whether the problem may be due to the microphone being disabled on the device itself.

Speaker Settings Window

The *Speaker Settings* window lets you change basic settings for a speaker.

You access the *Speaker Settings* window from the Administrator window (see page 30): Selecti a speaker in the *Administrator* window's *Device Manager* section, then click the *Settings* button.

- ***Device name:*** Displays the name of the speaker. If required, you are able to overwrite the existing speaker name with a new one.

- ***Enabled:*** Lets you enable/disable use of the speaker.

Tip: You can also enable/disable an audio source in the *Administrator* window (see page 30): Right-click the required audio source in the *Administrator* window's *Device Manager* section, then select *Disable* or *Enable* from the menu that appears.

Note: On some devices, a speaker can also be enabled/disabled on the device itself, typically through the device's own configuration web page. If a speaker on a device does not work after enabling it in the *Administrator* application, you should thus verify whether the problem may be due to the speaker being disabled on the device itself.

Recording Server Service Management

Using the Recording Server Manager

The Recording Server service is a vital part of the surveillance system; video streams are only transferred to XProtect Enterprise while the Recording Server service is running.

The Recording Server Manager informs you about the state of the Recording Server service. It also lets you manage the service.

A notification area (a.k.a. system tray) icon indicates whether the Recording Server service is running or not. Green indicates running (default), red indicates not running.

By right-clicking the icon you can start and stop the Recording Server service, view log files, etc.

Starting and Stopping the Recording Server

To start the Recording Server service, do the following:

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Start Recording Server Service.*
3. The icon changes to green.

To stop the Recording Server service, do the following:

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Stop Recording Server Service.*
3. The icon changes to red.

Opening the Administrator Application

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Open Administrator*.

Monitoring System Status

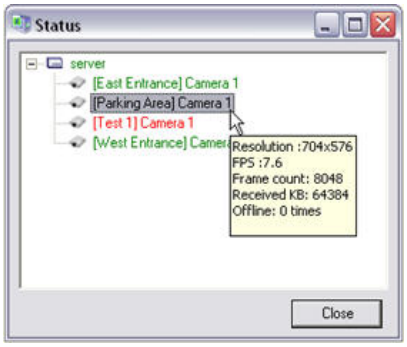
By right-clicking the notification area's Recording Server icon and then selecting *Show System Status*, you get access to the *Status* window. Alternatively, simply double-click the icon.

The *Status* window lets you view the status of the image server(s) and connected cameras. The status of each server/camera is indicated by a color:

- ***Green*** indicates that the server or camera is running correctly.

- ***Gray*** indicates that the *camera* (not the server) is not running. Typically, a camera will be indicated in gray in the following situations:
    - The camera has been set offline in the *Camera/Alert Scheduler* window (see page 71)
    - The Recording Server service has been paused from the *Service Manager* window (see page 70)
    - The Recording Server service has been stopped.
- ***Red*** indicates that the server or camera is not running. This may because it has been unplugged or due to a network or hardware. Errors are listed in the Recording Server log file (see the following).

By placing your mouse pointer over a camera icon in the status window, you will see detailed information about the camera in question. The information is updated approximately every 10 seconds.



- ***Resolution*:** Shows the resolution of the camera.
- ***FPS*:** Shows the number of frames per second (i.e. the frame rate) currently used by the camera. The number updates each time the camera has received 50 frames.
- ***Frame count*:** Shows the number of frames received from the camera since the Recording Server service was last started.
- ***Received KB*:** Shows the number of kilobytes sent by the by camera since the Recording Server service was last started.
- ***Offline*:** Indicates the number of times the camera has been offline due to an error.

Viewing Recording Server & Image Server Log Files

To view the recording server log file, do the following:

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Open Recording Server Log File...*

To view the Image Server log file, do the following:

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Open Image Server Log File...*

For more information about log files, see page 157.

Accessing the Built-in Help System

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Help*.

Viewing Information about Your XProtect Enterprise Version

1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *About...*

Knowing the version number can be useful in case you require support from your Milestone vendor.

Exiting the Recording Server Manager

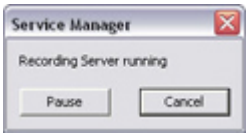
1. Right-click the notification area's Recording Server icon.
2. In the menu that appears, select *Exit Recording Server Manager.*

Tip: To re-open the Recording Server Manager, go to Windows' start menu and select *All Programs > Startup > Milestone XProtect Enterprise Recording Server Manager.*

Service Manager Window

The *Service Manager* window lets you pause/resume the Milestone Recording Server service. Pausing the service is necessary in order to access some features, such as configuration of PTZ (Pan/Tilt/Zoom) cameras. You access the *Service Manager* window by clicking the *Service Manager...* button in the *Administrator* window (see page 30).

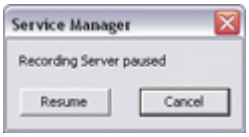
Pausing the Milestone Recording Server Service



To pause the Milestone Recording Server service, click the *Pause* button.

IMPORTANT: While the Milestone Recording Server service is paused, no video or audio will be available; neither for live viewing, nor for recording.

Resuming the Milestone Recording Server Service



When the service is paused, the *Service Manager* window closes. The next time you open it, the *Pause* button will have changed to *Resume*. Simply click the *Resume* button to resume the Milestone Recording Server service.

Tip: The service is automatically resumed when you exit the *Administrator* application.

What to Do if the Milestone Recording Server Service is Stopped

If the *Service Manager* window informs you that the recording server is stopped, the Milestone Recording Server service has been stopped (as opposed to paused) outside the *Administrator* application, possibly through the Recording Server Manager (see page 68). You are able to start a stopped Milestone Recording Server service through the Recording Server Manager.

Scheduling

Camera/Alert Scheduler Window

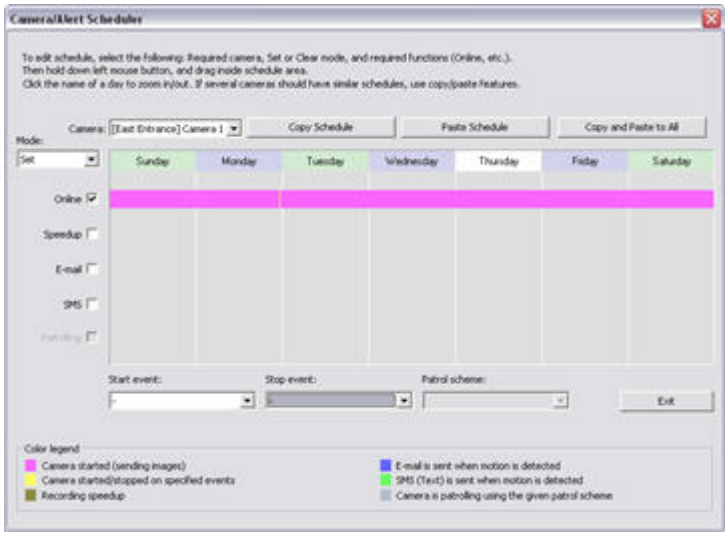
The *Camera/Alert Scheduler* window lets you specify when each camera should be online. A camera is online when it is transferring video to the XProtect Enterprise server for processing.

IMPORTANT: The fact that a camera is online (i.e. transferring video to the XProtect Enterprise server) will not necessarily mean that video from the camera is recorded (i.e. stored in the camera's database on the XProtect Enterprise server). Storage settings for individual cameras are specified in the *Camera Settings for [Device Name] [Camera Name]* Window (see page 43).

You are able to specify whether cameras should be online within specific periods of time, or whether they should start and stop transferring video when specific events occur within specific periods of time. You are also able to specify when the camera should speedup recording and if e-mail alerts or SMS alerts should be triggered if motion is detected during specific periods of time. If using PTZ cameras with patrolling, you are furthermore able to specify if certain patrol schemes should be used during specific periods of time.

By default, cameras added to XProtect Enterprise will automatically be online, and you will only need to modify the *Camera/Alert Scheduler* window's settings if you require cameras to be online only at specific times or events, or if you want to use specific alerts or PTZ patrol schemes.

Note, however, that this default may be changed by clearing the *General Settings* window's *Create Default schedule for new cameras* check box (see page 76): If the check box is cleared, subsequently added cameras will not automatically be online, in which case online schedules must be specified manually.



To access the *Camera/Alert Scheduler* window, click the *Scheduler...* button in the *Administrator* window (see page 30).

Camera/Alert Scheduler Window's Fields and Check Boxes

Field, Check Box	Description
Camera	Lets you select a particular camera, for which to specify or view a schedule in the window's calendar section. **Note:** Always verify that you have selected the required camera in the list;

Field, Check Box	Description
	even though schedules displayed in the calendar section may look—and indeed sometimes be—similar, the displayed schedule refers specifically to the selected camera.
Mode	Select whether to add or delete periods in the calendar section: • ***Set*:** Add periods. May also be used to overwrite existing periods. • ***Clear*:** Delete existing periods.
Online	Check the *Online* box when you want to set or clear online periods for the selected camera.
Speedup	Check the *Speedup* box when you want to set or clear when the camera should always/never speedup recording. **Note:** The *Speedup* check box is only available if you have enabled speedup in the *Camera Settings for [Device Name] [Camera Name]* window (see page 43).
E-mail	Check the *E-mail* box when you want to set or clear periods with motion- or database-related e-mail alerts for the selected camera. Such alerts can automatically be sent to one or more recipients when motion or database events are detected. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 80).
SMS	Check the *SMS* box when you want to set or clear periods with motion- or database-related SMS (mobile phone text message) alerts for the selected camera. Such alerts can automatically be sent to one or more recipients when motion or database events are detected. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).
Patrolling	Check the *Patrolling* box when you want to set or clear periods with patrolling for a selected PTZ (Pan/Tilt/Zoom) camera. **Note:** The *Patrolling* box is only available if you have selected a PTZ camera for which at least one patrol scheme has been set up.
Start event	When you set an *Online* period, you will be asked whether you want the selected camera to transfer video to the XProtect Enterprise software continuously within the specified period (*Always*), or only when an event occurs within the specified period (*On Event*). If using *On Event*, the *Start event* list lets you select the required start event. **Note:** The use of event-based online periods requires that events have been defined. Read more about events in *About Input, Events & Output ...* on page 84.

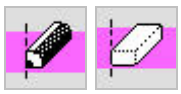
Field, Check Box	Description
Stop event	When you set an *Online* period, you will be asked whether you want the selected camera to transfer video to the XProtect Enterprise software continuously within the specified period (*Always*), or only when an event occurs within the specified period (*On Event*). If using *On Event*, the *Stop event* list lets you select the required stop event. **Note:** The use of event-based online periods requires that events have been defined. Read more about events in *About Input, Events & Output ...* on page 84.
Patrol scheme	When you set a *Patrolling* period for a PTZ camera with patrolling, the *Patrol scheme* list lets you select the required patrol scheme. N**ote:** The *Patrol scheme* list is only available if you have selected a PTZ camera for which at least one patrol scheme has been set up.

Camera/Alert Scheduler Window's Calendar Section

The *Camera/Alert Scheduler* window's calendar section lets you specify exact periods of time for each option for each camera selected in the window's *Camera* list.

Set and Clear Modes

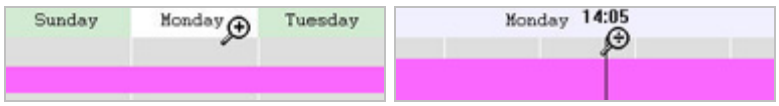
Depending on your selection in the *Mode* list, you *Set* or *Clear* periods in the calendar. Your selection is indicated by your mouse pointer turning into either a pencil (*Set*) or an eraser (*Clear*) when inside the calendar section.



Zoom Feature

When placing your mouse pointer inside the day band in the top part of the calendar section you get access to the calendar's zoom feature. With the zoom feature you are able to toggle between the calendar's default seven-day view and a single-day view.

The single-day view provides you with five-minute interval indications, allowing you to specify periods precisely.



Zoom feature allows you to toggle between seven-day and single-day views

How to Set or Clear Periods in the Calendar

To set or clear a period in the *Camera/Alert Scheduler* window's calendar section, simply click at the required start point in the calendar, and drag to set/clear a period (depending on whether you have selected *Set* or *Clear* in the window's Mode list).

Good to Know when You Set Online Periods

When you set an *Online* period, you will be asked whether you want the selected camera to transfer video to the XProtect Enterprise software continuously within the specified period (*Always*), or only when an event occurs within the specified period (*On Event*).

If using *On Event*, remember to specify required start and stop events in the *Start event* and *Stop event* lists.

Good to Know when You Set Patrolling Periods

Select the required patrol scheme from the *Patrol scheme* list, located below the calendar section, then drag to select the required period in the calendar. The *Patrol scheme* list is only available if you have selected a PTZ camera for which at least one patrol scheme has been set up.

When you set a *Patrolling* period, you may be able to select between several patrol schemes. This will depend upon how many patrol schemes have been set up in the *Setup PTZ Patrolling* window (see page 60).

If you set patrolling periods with different patrol schemes immediately following each other in time, changes between patrolling schemes will be indicated by a thin vertical line (see also *Colored Bars* in the following).

Colored Bars

The calendar uses colored bars to indicate active periods for each option (*Online*, *E-mail*, *SMS*, etc.):

- In the *Online* bar, active periods are indicated in either pink or yellow:
  - Pink (●) indicates that the selected camera is continuously transferring video to the XProtect Enterprise software.
  - Yellow (●) indicates that the selected camera transfers video to the XProtect Enterprise software when a specified event occurs.
- In the *Speedup* bar, active periods are indicated by olive green (●).
- In the *E-mail* bar, active periods are indicated in blue (●).
- In the *SMS* bar, active periods are indicated in green (●).
- In the *Patrolling* bar, active periods are indicated in gray (●). Changes between patrolling schemes are indicated by a thin vertical line. Note that the *Patrolling* bar is only available if you have selected a PTZ camera for which patrolling has been set up.

  Tip: When several patrol schemes are in use, you are able to see which patrol scheme is used for a particular period: Click the relevant section of the gray bar; the name of the patrol scheme in question will appear in the *Patrol scheme* list, located below the calendar section.

How to Copy and Paste Schedules

With the following buttons, you are able to copy and paste schedules, and thus save yourself considerable time:

Button	Description
Copy Schedule	Lets you copy the schedule displayed in the calendar section. When used in combination with the *Paste Schedule* button, you are able to quickly re-use

Button	Description
	schedules from one camera to another.
Paste Schedule	Lets you paste a copied schedule for use with the selected camera. The same copied schedule can be pasted to several cameras simply by selecting and pasting to, one camera after the other. **Tip:** If you want to use a schedule for all cameras, specify a schedule for one camera, then use the *Copy and Paste to All* button to copy the schedule and paste it to all cameras in one go.
Copy and Paste to All	Lets you copy the schedule displayed in the calendar section and paste it to all cameras in one go.

General Settings

General Settings Window

The *General Settings* window lets you manage a variety of settings, such as user rights, e-mail and SMS settings, logging, etc. To access the *General Settings* window, click the *General Settings...* button in the *Administrator* window (see page 30).

Administrator Settings

The *Administrator Settings* section lets you password protect access to the *Administrator* application. When the *Enable Protection* check box is selected, users must supply the administrator password in order to be able to access the *Administrator* application, and in order to be able to use any of the features to which access has been restricted.

Changing the Administrator Password

To change the administrator password, click the *Change Password...* button to open the *Change Password* window (see page 79). When an administrator password is in use, users accessing the *Administrator* application, or wishing to use protected features, must type the administrator password in the window before access is granted.

Manual Start Recording Settings

In the *Manual start recordings settings* section you can enable the possible to manually start recording in the Smart Client (see page 175). Select the check box *Enable manual start recording* to enable manually start of recording.

In the *Default duration of manual recording [secs.]:* field you can specify the number of seconds the recording should last. Note that the minimum number of seconds you can specify is 30.

The *Maximum duration of manual recording [secs.]:* field is reserved for future use.

Milestone XProtect Central Settings

Note: Settings in this section are relevant only if you are using Milestone XProtect Central (add-on product that provides complete overview of surveillance system status and alarms) in connection with XProtect Enterprise.

The *Milestone XProtect Central* section lets you enable and configure access to the surveillance system from a Milestone XProtect Central server in order to retrieve status information and alarms. To enable access from a Milestone XProtect Central server, select the *Enable Milestone XProtect Central connections* check box, and click the *Settings...* button to open the *Milestone XProtect Central Settings* window (see page 79), in which you specify which login settings the Milestone

XProtect Central server should use in order to access the surveillance system. The *Enable Milestone XProtect Central connections* check box is by default selected.

Patrolling Settings

Settings in this section are relevant only if you are using PTZ cameras for which patrolling has been set up. The regular patrolling of PTZ cameras may be interrupted, either manually or when a particular event occurs. The *Patrolling settings* section lets you specify how many seconds should pass before the regular patrolling is resumed after a manual or event-based interruption. Default is 30 seconds. The settings in this section will apply for all installed PTZ cameras.

IMPORTANT: Users of the Smart Client (see page 175) are—in addition to manual control—able to stop a selected PTZ camera's patrolling entirely. This takes place through a context menu in the Smart Client view. Therefore, for Smart Client users, the number of seconds specified in the *Patrolling settings* section does only apply when users manually control a PTZ camera; not when users stop a PTZ camera's patrolling entirely. When Smart Client users stop a PTZ camera's patrolling entirely, the camera's patrolling will resume only when the Smart Client user selects to resume it.

Tip: PTZ patrolling for individual PTZ cameras is configured in the *Setup PTZ Patrolling* window (see page 60).

Logfile Settings

The *Logfile Settings* section lets you specify where to keep the general log files containing information about activity in the *Administrator* and the *Recording Server* (see page 68), and for how long. Separate log files are generated for the *Administrator* and *Recording Server* service.

Logfile Path

By default, the *Administrator* and *Recording Server* log files are stored in the folder containing the XProtect Enterprise software, typically C:\Program Files\Milestone\Milestone Surveillance\. To specify another location for your log files, type the path to the required folder in the *Logfile Path* field, or click the browse button next to the field to browse to the required folder.

Days to Log

A new log file is created every day. A log file older than the number of days specified in the *Days to log* field is automatically deleted. By default, the log file will be stored for five days. To specify another number of days, simply overwrite the value in the *Days to log* field. The current day's activity is always logged, even with a value of *0* in the *Days to log* field. The maximum number of days to log is *9999*.

Tip: Read more about logging on page 157.

Event Recording Settings

As opposed to the general log files, which contain information about activity on the surveillance system itself, event log files contain information about registered events (for more information about events, see *About Input, Events & Output ...* on page 84). The *Event Recording Settings* section lets you specify where to keep event log files, and for how long. Event log files should be viewed using the *Smart Client* (see page 175) or *Viewer (*see page 169):

- ***Smart Client*:** In the Browse tab's *Alerts* section, select the required event, then click the *Get List* button to see when the event in question was detected.

- ***Viewer*:** Select the *Viewer*'s Alarm Overview control panel, then click the *Events* button to view the events log.

Path

By default, event log files are stored in the folder containing the XProtect Enterprise software, typically C:\Program Files\Milestone\Milestone Surveillance\. To specify another location for your log files, type the path to the required folder in the *Path* field, or click the browse button next to the field to browse to the required folder.

Days to Keep

A new event log file is created every day. Event log files older than the number of days specified in the *Days to keep* field are automatically deleted. By default, event log files will be stored for five days. To specify another number of days, simply overwrite the value in the *Days to keep* field. The current day's activity is always logged, even with a value of *0* in the *Days to keep* field. The maximum number of days to log is *9999*.

Tip: Read more about logging on page 157.

Advanced

Check Box	Description
Don't send e-mail on camera failures	If selected, no e-mail alerts will be sent if XProtect Enterprise loses contact with a camera. Otherwise, e-mail alerts will, provided the e-mail alert feature has been enabled in the *E-Mail setup* window (see page 80), automatically be sent if XProtect Enterprise loses contact with a camera, regardless of any e-mail alerts periods defined in the *Camera/Alert Scheduler* window (see page 71).
Don't send SMS on camera failures	If selected, no SMS alerts will be sent if XProtect Enterprise loses contact with a camera. Otherwise, SMS alerts will, provided the SMS alert feature has been enabled in the *SMS settings* window (see page 82), automatically be sent if XProtect Enterprise loses contact with a camera, regardless of any e-mail alerts periods defined in the *Camera/Alert Scheduler* window (see page 71).
Start cameras on remote live requests	Cameras may be stopped, for example because they have reached the end of an online schedule (see page 71), in which case *Remote Client* (see page 178) and *Smart Client* (see page 175) users will not be able to view live video from the cameras. However, if *Start cameras on remote live requests* is selected, Remote Client and Smart Client users will be able to start the camera in order to view live video from the camera.
Create default schedule for new cameras	If selected (default), a schedule specifying that the camera is always online (i.e. transferring video to XProtect Enterprise) will automatically be created in the *Camera/Alert Scheduler* window (see page 71). The automatically created schedule can be edited manually at any time. If not selected, no schedule will automatically be created; meaning that the

Check Box	Description
	camera will not automatically be transferring video to XProtect Enterprise. When required, schedules can be added manually in the *Camera/Alert Scheduler* window (see page 71).

Email Settings

Clicking the *Email Settings...* button opens the *E-Mail setup* window (see page 80), in which you enable and configure the use of e-mail alerts.

Sms Settings

Clicking the *Sms Settings...* button opens the *SMS settings* window (see page 82), in which you enable and configure the use of SMS (mobile phone text message) alerts.

Note: Use of the SMS alert feature requires that an external Siemens TC-35 GSM modem has been attached to a serial port on the computer running the XProtect Enterprise software.

Change Password Window

The *Change Password* window lets you change the administrator password for your XProtect Enterprise solution. To access the *Change Password* window, click the *Change Password...* button in the *General Settings* window (see page 76).

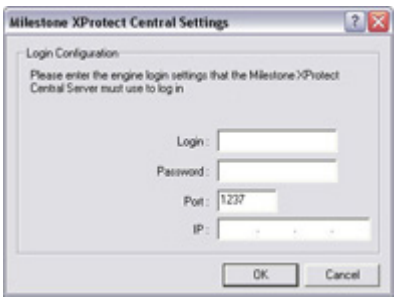
How to Change the Administrator Password

1. Specify the current administrator password in the *Old password* field
2. Specify the new administrator password in the *New password* field
3. Repeat the new administrator password in the *New password (confirm)* field
4. Click *OK*.

Milestone XProtect Central Settings Window

Note: Settings in the *Milestone XProtect Central Settings* window are relevant only if you are using the Milestone XProtect Central add-on product in connection with XProtect Enterprise.

The *Milestone XProtect Central Settings* window lets you specify the login settings required for a Milestone XProtect Central server to access the surveillance system in order to retrieve status information and alarms. To access the *Milestone XProtect Central Settings* window, click the *Settings...* button in the *Milestone XProtect Central Settings* section of the *General Settings* window (see page 76).



Specify login settings for the Milestone XProtect Central server in the following fields:

- ***Login*:** Type the name of the XProtect Enterprise server. The name must match the name specified on the Milestone XProtect Central server itself. Default name is *Name*.
- ***Password*:** Type the password used for accessing the XProtect Enterprise server. The password must match the password specified on the Milestone XProtect Central server itself. Default password is *Pass*.
- ***Port*:** Type the port number to which the Milestone XProtect Central server should connect when accessing the XProtect Enterprise server. The port number must match the port number specified on the Milestone XProtect Central server itself. Default port is 1237.
- ***IP*:** When the Milestone XProtect Central server retrieves alarms from the XProtect Enterprise server, the XProtect Enterprise server includes information about its IP address in the alarm information. If the Milestone XProtect Central server accesses the XProtect Enterprise server over the internet, or if the XProtect Enterprise server has two or more network adapters, you must specify the IP address to which the Milestone XProtect Central server should connect. If you do not specify an IP address, the IP address of the first network adaptor found the XProtect Enterprise server will be used.

E-Mail Setup Window

The *E-Mail setup* window lets you enable and configure the use of e-mail alerts. Such e-mail alerts can automatically be sent to one or more recipients when motion is detected or specific events (see *About Input, Events & Output ...* on page 84) occur.

By default, SMTP (Simple Mail Transfer Protocol) is used when sending e-mail alerts. Compared with other mail transfer methods, SMTP has the advantage that you will avoid automatically triggered warnings from your e-mail client when an e-mail alert is to be sent. Such automatically triggered warnings may otherwise inform you that your e-mail client is trying to automatically send e-mail messages on your behalf.

To access the *E-Mail setup* window, click the *Email Settings...* button in the *General Settings* window (see page 76).

Enabling E-mail Alerts

You enable the use of e-mail alerts separately for the Milestone *Recording Server* (see page 68) and—if applicable—the *Viewer application (*see page 169):

Note: When enabling e-mail alerts, also consider the e-mail alert schedules configured for each camera in the *Camera/Alert Scheduler* window (see page 71).

- ***Enable E-Mail (Recording Server)*:** Select check box to enable the use of e-mail alerts when the Milestone *Recording Server* is running. E-mail alerts will then be sent when the following conditions apply:
  - the Milestone *Recording Server* is running
  - motion is detected or an event, for which the sending of an e-mail alert has been defined, occurs
  - motion is detected within a period of time for which an e-mail alert schedule has been defined
- ***Enable E-Mail (Viewer)*:** Select check box to enable the use of e-mail alerts in the *Viewer* application. In effect, this will display the *E-Mail Report* button in the *Viewer*'s toolbar,

enabling users to send evidence via e-mail. If you clear the check box, the *E-Mail Report* button will not be available in the *Viewer*'s toolbar.

Use of the e-mail feature is only possible when the *Viewer* is run on the surveillance system server itself; not in a *Viewer* exported with video evidence.

Specifying Recipients

You specify the e-mail addresses to which e-mail alerts should be sent in the *Recipient(s)* field. If specifying more than one e-mail address, separate the e-mail addresses with semicolons (example: aa@aa.aa;bb@bb.bb;cc@cc.cc).

Note: If e-mail alerts are enabled for the *Viewer*, the content you specify in the *Recipient(s)* field will appear as the default value in the *Viewer*'s dialog for sending evidence via e-mail. Users will be able to overwrite this default value.

Specifying Sender Settings

Note: SSL (Secure Socket Layer) is not supported; if the sender belongs on a server that requires SSL, the e-mail alerts will not work properly. Also, you may be required to disable any e-mail scanners that could prevent the application sending the e-mail alert.

- ***Sender e-mail address*:** Type the e-mail address you wish to appear as the sender of the e-mail alert.
- ***Outgoing mail (SMTP) server name*:** Type the name of the SMTP server which will be used for sending the e-mail alerts.
- ***Server requires login*:** Select check box if a user name and password is required to use the SMTP server.
- ***Username*:** Field available only when *Server requires login* is selected. Type the user name required for using the SMTP server.
- ***Password*:** Field available only when *Server requires login* is selected. Type the password required for using the SMTP server.

Specifying Default Subject and Message Texts

- ***Subject text*:** Specify required subject text for e-mail alerts.
- ***Message text*:** Specify required message text for e-mail alerts. Note that camera information as well as date and time information is automatically included in e-mail alerts.

Note: If e-mail alerts are enabled for the *Viewer*, the content you specify in the *Subject text* and *Message text* fields will appear as default values in the *Viewer*'s dialog for sending evidence via e-mail. Users will be able to overwrite these default values.

Specifying Image and Interval Options

You are able to specify whether e-mail alerts should include images, and how much time should pass between alerts per camera:

- ***Include Image*:** Select check box to include images in e-mail alerts. When selected, a JPG image from the time the triggering event occurred will be attached to each alert e-mail.

- ***Time btw. motion-related mails (minutes)*:** Specify required minimum time (in minutes) to pass between the sending of each e-mail alert per camera. Note that this interval only applies for e-mail alerts generated by detected motion or database-related events; e-mail alerts generated by other types of events will still be sent out whenever the events occur.

  Examples: If specifying *5*, a minimum of five minutes will pass between the sending of each motion- or database-related e-mail alert per camera, even if motion or database events are detected in between. If specifying *0*, e-mail alerts will be sent each time motion or database events are detected, potentially resulting in a very large number of e-mail alerts being sent. If using the value *0,* you should therefore consider especially the motion detection sensitivity configured for each camera in the *Adjust Motion Detection* window (see page 50).

Testing Your E-Mail Alert Configuration

You are able to test your e-mail alert configuration by clicking the *Test* button. This will send a test e-mail to the specified recipients. If *Include Image* is selected, the test e-mail will have a test JPG image attached.

SMS Settings Window

Note: Use of the SMS (mobile phone text message) alert feature requires that an external Siemens TC-35 GSM modem has been attached to a serial port on the computer running the XProtect Enterprise software.

The *SMS settings* window lets you enable and configure the use of SMS alerts. Such SMS alerts can automatically be sent to one or more recipients when motion is detected or specific events (see *About Input, Events & Output ...* on page 84) occur.

To access the *SMS settings* window, click the *Sms Settings...* button in the *General Settings* window (see page 76).

Enabling SMS Alerts

You enable the use of SMS alerts by selecting the *Enable SMS* check box.

Note: When enabling the use of SMS alerts, also consider the SMS alert schedules configured for each camera in the *Camera/Alert Scheduler* window (see page 71).

Specifying SMS Alert Settings

Having selected the *Enable SMS* check box, specify SMS alert settings in the following fields:

- ***GSM modem con. to*:** Select port connecting the computer running XProtect Enterprise to the GSM modem.

- ***SIM card PIN code*:** Specify PIN code for the SIM card inserted in the GSM modem.

- ***SIM card PUK code*:** Specify PUK code for the SIM card inserted in the GSM modem.

- ***SMS Central Phone No.*:** Specify the number of the SMS central to which the GSM modem should connect in order to send an SMS.

- ***Recipient Phone No.*:** Specify the number of the telephone to which SMS alerts should be sent.

- ***Message*:** Specify required message text for SMS alerts. Message text must be no longer that 100 characters, and must only contain the following characters: a-z, A-Z, 0-9 as well as commas (,) and full stops (.). Note that camera information as well as date and time information is automatically included in SMS alerts.

- ***Time btw. transmissions*:** Specify required minimum time (in minutes) to pass between the sending of each SMS alert per camera.

  Examples: If specifying *5*, a minimum of five minutes will pass between the sending of each SMS alert per camera, even if motion is detected or events occur in between. If specifying *0*, SMS alerts will be sent each time motion is detected or events occur, potentially resulting in a very large number of SMS alerts being sent. If using the value *0,* you should therefore consider the motion detection sensitivity configured for each camera in the *Adjust Motion Detection* window (see page 50).

Testing Your SMS Alert Configuration

You are able to test your SMS alert configuration by clicking the *Test* button. This will send a test SMS to the specified recipients.

Note: If the Milestone *Recording Server* service (see page 68) is running, the button will not be available. To make the button available, pause the Milestone *Recording Server* service by clicking the *Administrator* window's (see page 30) *Service Manager* button, then clicking the *Pause* button.

IMPORTANT: No video or audio will be recorded while the Milestone *Recording Server* service is paused.

Input, Events & Output

About Input, Events & Output …

Input received from a wide variety of sources can be used to generate events in XProtect Enterprise.

Events can in turn be used for automatically triggering actions in XProtect Enterprise, such as starting or stopping recording on cameras, triggering e-mail or SMS notifications, making PTZ cameras move to specific preset positions, making video automatically appear on Matrix (see page 135) recipients, etc. Events can also be used for activating output.

Output units can be attached to output ports on many devices, allowing you to activate lights, sirens, etc. from XProtect Enterprise. Such external output can be activated automatically by events, or manually from the Remote Client / Smart Client.

Types of Events

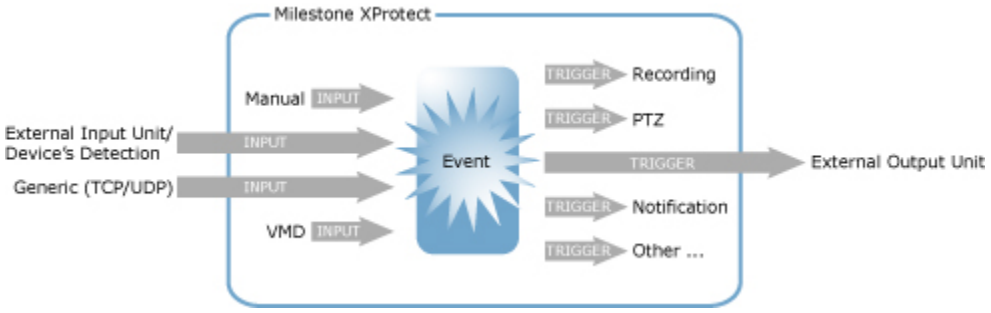
You specify which types of input should generate which types of events. Basically, four types of events exist:

- On many devices you are able to attach external input units to input ports on the device. Events based on input from such external input units—typically sensors attached to doors, windows, etc.—are called ***input events***. Some devices also have their own capabilities for detecting motion, for detecting moving and/or static objects, etc. (typically configured in the devices' own software), in which case you are also able to use such detections from the device as input events.

- Input may also be received in the form of TCP or UDP data packages, which can be analyzed and, if matching specified criteria, used to generate events. Such events are called ***generic events***.

- Events may be based on XProtect Enterprise detecting motion on a camera. Such events are called ***VMD (i.e. Video Motion Detection) events***.

- Finally, events may be generated manually by users selecting them in their access clients. Such manually selectable events are traditionally called ***event buttons***.



Events—whether based on manual input, based on input from external input units/devices' own detections, based on received TCP/UDP data packages, or based on Milestone XProtect Enterprise-detected motion—can trigger a wide variety of actions.

Specifying Input, Events and Output

In XProtect Enterprise, your main entry point for configuration of input, event and output handling is the *Administrator* window (see page 30:

- By clicking the *Administrator* window's *I/O Setup...* button, you open the *I/O Setup* window (see page 86), in which you are able to specify each individual ***input event***, ***VMD event*** and ***output***.

- By clicking the *Administrator* window's *Event Buttons...* button, you open the *Event Buttons* window (see page 96), in which you are able to specify ***event buttons*** for manually triggering events-controlled activity.

- By clicking the *Administrator* window's *Generic Events...* button, you open the *Generic Events* window (see page 100), in which you are able to specify ***generic events***.

- By clicking the *Administrator* window's *I/O Control...* button, you open the *I/O Control* window (see page 105), in which you are able to ***associate specific events with specific output***. This way you can, for example, specify that when motion is detected on a camera (typically specified as a VMD event) a siren should automatically sound (output). If you want users to be able to manually activate output when operating specific cameras, you specify this in the *Output Settings for [Device Name] [Camera Name]* window (see page 106).

Note: Before you specify use of external input and output units on a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the Milestone release notes to verify that input and output controlled operations are supported for the device and firmware used.

Note: If you are using several XProtect Enterprise servers in your surveillance solution setup, input and output on a specific device should be defined on one of the servers only. Do not define the same input or output on the same device on several servers. This applies even for dedicated I/O devices (see also Using Dedicated I/O Devices on page 85).

Using Dedicated I/O Devices

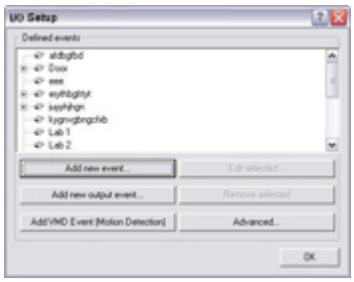
In addition to IP video camera devices and IP video encoder devices it is possible to add a number of dedicated I/O (input/output) devices to XProtect Enterprise (see How to Add a Device on page 36). For information about which I/O devices are supported, refer to the release note.

When such I/O devices are added, input on the I/O devices can be used to generate events in XProtect Enterprise, and events in XProtect Enterprise can be used for activating output on the I/O devices. This means that I/O devices can be used in your events-based system setup in the same way as a camera.

Note: When using some I/O devices it is necessary for the surveillance system to regularly check the state of the devices' input ports in order to detect whether input has been received. Such state checking at regular intervals is called *polling*. The interval between state checks, called a *polling frequency*, is specified in the *Advanced* window (see page 95). For such I/O devices, the polling frequency should be set to the lowest possible value (one tenth of a second between state checks). For information about which I/O devices require polling, see the release note.

I/O Setup

I/O Setup Window



You access the *I/O Setup* window by clicking the *I/O Setup...* button in the *Administrator* window (see page 30). The *I/O Setup* window lets you define input events, VMD (Video Motion Detection) events and output for devices on your surveillance system. When events occur, they can trigger one or more actions:

- *Input events* occur when input from an external input unit is received on a device's input port, for example when an external sensor detects that a door is opened. Some devices also have their own capabilities for detecting motion, for detecting moving and/or static objects, etc. (configured in the devices' own software; typically by accessing a browser-based configuration interface on the device's IP address), in which case such detections from the device can also be used as input events.

- *VMD events* occur when XProtect Enterprise detects motion on a particular camera.

- *Outputs* are used for activating external output units, for example for switching on lights or sounding a siren.

The *I/O Setup* window is used for defining which input events, VMD events and outputs should be available on your system. Input and VMD events can be used for triggering outputs or for triggering various actions on the surveillance system itself, such as for starting or stopping cameras (configured in the *Camera/Alert Scheduler* window – see page 71) or for moving a PTZ camera to a particular preset position (configured in the *Event* window (for PTZ preset positions on event) – see page 59).

Once you have defined input events, VMD events and outputs, you are able to associate specific input events or VMD events with specific outputs in the *I/O Control* window(see page 105), so that, for example, lights are switched on when a door is opened or when motion is detected on a camera. Outputs may also be triggered by motion detection on a specific camera—even without a defined VMD event—or manually through the Smart Client (see page 175); both are configured in the *Output Settings for [Device Name] [Camera Name]* window (see page 106).

Note: Before you specify inputs and outputs for a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check Milestone's release notes to verify that input and output controlled operations are supported for the device and firmware used.

Using the I/O Setup Window's Defined Events List and Buttons

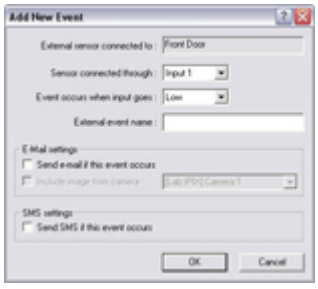
The *I/O Setup* window features a *Defined events* list, in which input, output and VMD (Video Motion Detection) events defined for each device are listed. The window furthermore features a number of buttons for use when adding and configuring the events:

Button	Description
Add new event...	Used for defining input events on the device selected in the *Defined events* list. Depending on the type of device, you may be able to define one or more input events on the device. Some devices do not support input/output at all. Refer to the release notes for device-specific information. **Devices Capable of Handling One Input Event Only** If the device is capable of handling one input event only, the button will open the *Add New Event* window (for devices capable of handling one input event

Button	Description
	only) – see page 88 – in which you define the input event, and any e-mail or SMS alerts to be associated with it. If you have already defined an input event on a device capable of handling one input event only, the *Add new event...* button will not be available when the device is selected in the *Defined events* list. However, if you click the plus sign next to the device in the *Defined events* list, and select the defined input event, the *Add new event...* button becomes available for defining timer events (see *Timer Events* in the following). **Devices Capable of Handling Several Input Events** If the device is capable of handling more than one input event, the button will open the *Multiple Input Events* window (see page 90), in which you define which of the device's possible input events should be enabled, and whether any alerts should be associated with enabled input events. **Timer Events** When you click the plus sign next to the device in the *Defined events* list, and select a defined input event, the *Add new event...* button becomes available for defining timer events: When clicked, the button will open the *New Timer* window (see page 93), in which you are able to specify the settings for timer events. Timer events are separate events, triggered by the input event under which they are defined. Timer events occur a specified number of seconds or minutes after the input event under which they are defined. Timer events may be used for a wide variety of purposes; the following are examples only: • A camera starts based on an input event, e.g. when a door is opened, a timer event stops the camera after 15 seconds • A camera starts and the lights are switched on based on an input event, e.g. when a door is opened, a timer event stops the camera after one minute, and another timer event switches the lights off after two minutes
Add new output event...	Opens the *Add New Output* window (see page 94), in which you are able to specify a name for the required output event, which of the device's output ports to use, and how long to keep the output for.
Add VMD Event (Motion Detection)	Lets you add a VMD (Video Motion Detection) event to the device selected in the *Defined Events* list. VMD events are events triggered when XProtect Enterprise detects motion on a specific camera, based on the motion detection settings defined in the *Adjust Motion Detection* window (see page 50). **Note:** In addition to XProtect Enterprise's motion detection, some devices also have their own capabilities for detecting motion (configured in the devices' own software; typically by accessing a browser-based configuration interface on the device's IP address). Events based on motion detected *on a device itself* are not VMD Events; they are input events, since they are based on input from the device. VMD events can be used just like regular input events. For example, a PTZ (Pan/Tilt/Zoom) camera could move to a specific preset position when a VMD event occurs. Only one VMD event can be defined per camera. In order to

Button	Description
	avoid the risk of an excessively high number of VMD events being generated, a VMD event cannot occur more frequently than every five seconds. The *Add VMD Event (Motion Detection)* button works slightly different depending on whether the selected device is a single-camera device or a multi-camera device, such as a video encoder: • ***Single-camera devices*:** Clicking the *Add VMD Event (Motion Detection)* button will instantly add a VMD event to the selected device, provided a VMD event has not already been defined for the device. • ***Multi-camera devices*:** Clicking the *Add VMD Event (Motion Detection)* button will open a simple dialog in which you select the required camera. This way you are able to define a VMD event for each camera on a multi-camera device.
Edit selected...	Lets you edit the settings for an item selected in the *Defined events* list. For devices capable of handling a single input event only, the button will open the *Edit Event* window (for editing input events) – see page 92. For devices capable of handling several input events, the button will open the *Multiple Input Events* window (see page 90). If the selected item is a timer event, the button will open the *New Timer* window (see page 93). If the selected item is an output, the button will open the *Edit Output* window (see page 94).
Remove selected	Lets you remove an event selected in the *Defined events* list. **Note:** The selected event will be removed without further warning.
Advanced...	Opens the *Advanced* window (see page 95), in which you are able to specify network settings to be used in connection with event handling: which ports to use for FTP, alerts and SMTP input/output events as well as which polling frequency to use on devices requiring polling.

Add New Event Window (for Devices Capable of Handling One Input Only)



The *Add New Event* window (for devices capable of handling one input event only) lets you specify the settings for an input event on devices capable of handling one input event only.

You access the *Add New Event* window (for devices capable of handling one input event only) by selecting the required device and clicking the *Add new event...* button in the *I/O Setup* window (see page 86). Note that this only applies when the selected device is capable of handling a single input event only. Some devices are capable of handling several

input events, in which case a different window, the *Multiple Input Events* window (see page 90), will open when the *Add new event...* button is clicked.

Note: Before you specify input events for a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the XProtect Enterprise release note to verify that input-controlled operations are supported for the device and firmware used.

Add New Event Window's Fields

The *Add New Event* window (for devices capable of handling one input event only) contains the following fields:

Field, Check Box	Description
External sensor connected to	Read-only field, displaying the name of the device on which the input event is defined.
Sensor connected through	Lets you select which of the device's input ports the sensor used for the input event is connected to.
Event occurs when input goes	Lets you select whether input event should be triggered when the signal on the input sensor rises or falls: • ***Low*:** Trigger input event when the signal on the sensor is falling • ***High*:** Trigger input event when the signal on the sensor is rising For exact information about what constitutes a falling and a rising signal respectively, refer to documentation for the sensor and device in question.
External event name	Lets you specify a name for the input event. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]. Some camera devices only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Send e-mail if this event occurs	Select check box to send an e-mail alert when the input occurs. In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 80).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the input event is triggered, in the e-mail alert, then select the required camera in the list next to the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the input occurs. In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).

Multiple Input Events Window

The *Multiple Input Events* window is used for devices capable of handling several input events. It lets you define which of the device's possible input events should be enabled, and whether any alerts should be associated with enabled input events.

Note: Before you specify input events for a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check Milestone's release notes to verify that input and output controlled operations are supported for the device and firmware used.

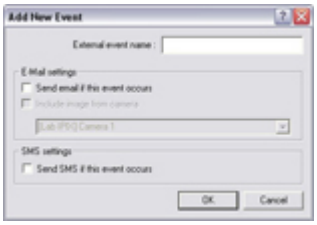
You access the *Multiple Input Events* window by clicking the *Add new event...* button in the *I/O Setup* window (see page 86). Note that this only applies when the device selected in the *I/O Setup* window is capable of handling several input events. Some devices are capable of handling a single input event only, in which case a different window, the *Add New Event* window (for devices capable of handling one input event only) – see page 88, will open when the *Add new event...* button is clicked.

Multiple Input Events Window's Fields and Buttons

Field, Button	Description
Input events for device	Read-only field, displaying the name of the device on which the input events are defined.
Available Input Event(s)	Lists available input events for the device, typically with an input event for rising and falling signals on each of the device's input ports. For exact information about what constitutes the various input events, refer to documentation for the sensors and device in question. **My list contains event related to motion and/or object detection; what's this?** Some devices have their own capabilities for detecting motion and/or moving/static objects. A motion or object detection-related input event is very likely to be an option from such a device. The settings determining this kind of detection are configured on the device itself; typically by accessing a browser-based configuration interface on the device's IP address. For more information, refer to the documentation for the device in question.
Enabled Input Event(s)	Lists enabled input events for the device. You enable an event by selecting it in the *Available Input Event(s)* list, then clicking the >> button. See description in the following.
>>	You enable an event by selecting it in the *Available Input Event(s)* list, then clicking the >> button to open the *Add New Event* window (for devices capable of handling several input events) – see page 91 – in which you specify a name for the input event, and any e-mail or SMS alerts to be associated with it. When you click *OK* in the *Add New Event* window (for devices capable of handling several input events), the selected input event is automatically transferred from *Available Input Event(s)* list to the *Enabled Input Event(s)* list.
<<	Lets you move an input event selected in the *Enabled Input Event(s)* list to the *Available Input Event(s)* list, thus disabling it.

Field, Button	Description
Edit	Lets you edit the settings for an input event selected in the *Enabled Input Event(s)* list.

Add New Event Window (for Devices Capable of Handling Several Inputs)



The *Add New Event* window (for devices capable of handling several input events) lets you specify the settings for a particular input event on devices capable of handling several input events. You access the *Add New Event* window (for devices capable of handling several input events) by clicking the >> button in the *Multiple Input Events* window (see page 90).

Note: Before you specify input events for a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check Milestone's release notes to verify that input and output controlled operations are supported for the device and firmware used.

Add New Event Window's Fields

The *Add New Event* window (for devices capable of handling several input events) contains the following fields:

Field, Check Box	Description
External event name	Lets you specify a name for the particular input event. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]. Some camera devices only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Send email if this event occurs	Select check box to send an e-mail alert when the input occurs. In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 80).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the input event is triggered, in the e-mail alert, then select the required camera in the list below the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the input occurs. In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).

Edit Event Window (for Editing Input Events)

The *Edit Event* window (for editing input events) lets you edit the settings for an existing input event on devices capable of handling one input event only. You access the *Edit Event* window (for editing input events) by selecting the required device and clicking the *Edit selected...* button in the *I/O Setup* window (see page 86). Note that this only applies when the selected device is capable of handling a single input event only. Some devices are capable of handling several input events, in which case a different window, the *Multiple Input Events* window (see page 90), will open when the *Edit selected...* button is clicked.

Edit Event Window's Fields

The *Edit Event* window (for editing input events) contains the following fields:

Field	Description
External sensor connected to	Read-only field, displaying the name of the device on which the input event is defined.
Sensor connected through	Lets you select which of the device's input ports the sensor used for the input event should be connected to.
Event occurs when input goes	Lets you select whether the input event should be triggered when the signal on the input sensor rises or falls: • ***Low*:** Trigger input event when the signal on the sensor is falling • ***High*:** Trigger input event when the signal on the sensor is rising For exact information about what constitutes a falling and a rising signal respectively, refer to documentation for the sensor and device in question.
External event name	Lets you edit the name of the input event. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]. Some camera devices only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Send e-mail if this event occurs	Select check box to send an e-mail alert when the input occurs. In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 80).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the input event is triggered, in the e-mail alert, then select the required camera in the list next to the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the input occurs. In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).

New Timer Window

The *New Timer* window lets you specify the settings for timer events. Timer events are separate events, triggered by the input event, VMD event, generic event or event button under which they are defined. Timer events occur a specified number of seconds or minutes after the event under which they are defined has occurred or the event button under which they have been defined has been clicked.

Timer events may be used for a wide variety of purposes; the following are examples only:

- A camera starts recording based on an input event, e.g. when a door is opened; a timer event stops the recording after 15 seconds
- Lights are switched on and a camera starts recording based on a VMD event, i.e. when motion is detected; a timer event stops the recording after one minute, and another timer event switches the lights off after two minutes

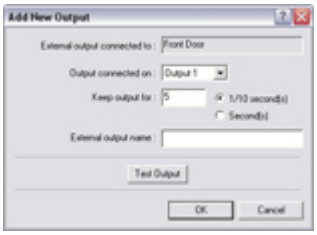
You are able to access the *New Timer* window in three ways:

- If dealing with input and VMD events in the *I/O Setup* window (see page 86): When you click the plus sign (⊞) next to a device in the window's *Defined events* list, and select a defined event, you are able to click the *Add new event...* button to access the *New Timer* window.
- If dealing with event buttons in the *Event Buttons* window (see page 96): When selecting an already specified event button in the *Defined Events* list, you are able to click the *Add new event...* button to access the *New Timer* window.
- If dealing with TCP- and/or UDP-based events in the *Generic Events* window (see page 100): When selecting an already specified event in the *Defined Events* list, you are able to click the *Add new event...* button to access the *New Timer* window.

New Time Window's Fields

Field	Description
Timer event is started by	Read-only field, displaying the name of the event or event button under which the timer event is defined.
Timer event name	Lets you specify a name for the timer event. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]. Some camera devices only support event names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.
Timer event occurs after	Lets you specify the amount of time that should pass between the event occurring/event button being clicked and the timer event. Specify the required amount of time in either seconds or minutes. Example: • The timer event should occur 15 seconds after the event under which it is defined has occurred • The timer event should occur 2 minutes after the event button under which it has been defined has been clicked

Add New Output Window



The *Add New Output* window lets you specify the settings for an output on a device. You access the *Add New Output* window by selecting the required device and clicking the *Add new output event...* button in the *I/O Setup* window (see page 86). If the device does not support output, the button will not be available.

Note: Before you specify output for a device, verify that the output is supported by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the XProtect Enterprise release note to verify that output is supported for the device and firmware used.

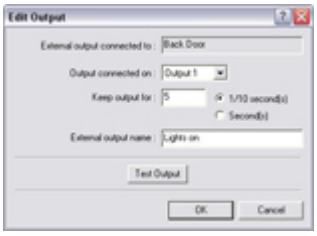
Add New Output Window's Fields

Field	Description
External output connected to	Read-only field, displaying the name of the device on which the output event is defined.
Output connected on	Lets you select which of the device's output ports the output is connected to. Many cameras only have a single output port; in that case simply select *Output 1*.
Keep output for	Lets you specify the amount of time for which the output should be applied. Specify the required amount of time in either 1/10 seconds or seconds.Example: The output should be kept for five tenths of a second. **Note:** Some devices are only able to apply outputs for a relatively short time, for example max. five seconds. Refer to the documentation for the device in question for exact information.
External output name	Lets you specify a name for the output. The name will appear on the button/list with which users will be able to manually trigger the output. **Note:** Output names must not contain the following characters: < > & ' " \ / : * ? | [ ]. Some camera devices only support output names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.

Testing the Defined Output

When you have defined settings for the output in question, you are able to test the output by clicking the *Test Output* button.

Edit Output Window



The *Edit Output* window lets you specify the settings for an output on a device. You access the *Edit Output* window by selecting the required output in the *I/O Setup* window (see page 86), then clicking the *Edit selected...* button.

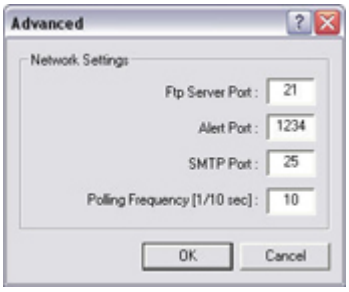
Edit Output Window's Fields

Field	Description
External output connected to	Read-only field, displaying the name of the device on which the output event is defined.
Output connected on	Lets you edit which of the device's output ports the output is connected to.
Keep output for	Lets you edit the amount of time for which the output should be applied. Specify the required amount of time in either 1/10 seconds or seconds. Example: The output should be kept for five tenths of a second. **Note:** Some devices are only able to apply outputs for a relatively short time, for example max. five seconds. Refer to the documentation for the device in question for exact information.
External output name	Lets you edit the name of the output. **Note:** Output names must not contain the following characters: < > & ' " \ / : * ? | [ ]. Some camera devices only support output names of a certain length and/or with a certain structure. Refer to the camera's documentation for exact details.

Testing the Defined Output

When you have defined settings for the output in question, you are able to test the output by clicking the *Test Output* button.

Advanced Window



The *Advanced* window lets you specify network settings to be used in connection with event handling. You access the *Advanced* window by clicking the *Advanced...* button in the *I/O Setup* window (see page 86).

Port Numbers and Polling Frequency

Field	Description
Ftp Server Port	Lets you specify port number to use for sending event information from the device to the surveillance system via FTP. Default port is port 21.
Alert Port	Lets you specify port number to use for handling event-based alerts, including generic events (see page 100). Default port is port 1234.
SMTP Port	Lets you specify port number to use for sending event information from the device to the surveillance system via SMTP. Default port is port 25.

Field	Description
Polling Frequency [1/10 sec]	For a small number of devices, primarily I/O devices (see Using Dedicated I/O Devices on page 85), it is necessary for the surveillance system to regularly check the state of the devices' input ports in order to detect whether input has been received. Such state checking at regular intervals is called *polling*. The *Polling Frequency* field lets you specify the interval between state checks. Interval is specified in tenths of a second. Default value is 10 tenths of a second (i.e. one second). For I/O devices it is highly recommended that the polling frequency is set to the lowest possible value (one tenth of a second between state checks). For information about which devices require polling, see the release note.

Event Buttons

What Is an Event Button?

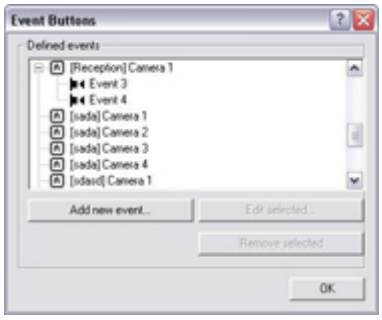
Event buttons lets users manually trigger events from the Smart Client (see page 175). In the Smart Client, event buttons are actually not buttons; instead users manually trigger events by selecting them from a list.

You are able to configure event buttons to suit the exact needs of your organization. Your main entry point for configuring event buttons is the *Administrator* window (see page 30): Clicking the *Administrator* window's *Event Buttons...* button will open the *Event Buttons* window (see below), in which you specify each individual event button.

Event buttons can be used for a wide variety of purposes, for example:

- As start and stop events for use in the *Camera/Alert Scheduler* window (see page 71). For example, you can make a camera start or stop transferring video to the surveillance system when an event button is selected.
- As start and stop events for use in the *Camera Settings for [Device Name] [Camera Name]* window (see page 43). For example, you can make a camera use a higher frame rate when an event button is selected, or you can use an event button for manually triggering PTZ preset positions on event (see page 59).
- For triggering outputs. Particular outputs can be associated with the clicking of an event button; you do this in the *I/O Control* window (see page 105).
- For triggering event-based e-mail and/or SMS alerts.
- In combinations. For example, the clicking of an event button could make a camera start transferring video to the surveillance system while two outputs are triggered and an e-mail alert is sent to relevant people.

Event buttons can be global (available for all cameras) or tied to a particular camera (only available when the camera in question is selected).



Event Buttons Window

The *Event Buttons* window lets you specify event buttons. When specified, event buttons become available in the Smart Client – see page 175 (in the Smart Client, event buttons are actually not

buttons; instead users manually trigger events by selecting them from a list). Event buttons can be global (available for all cameras) or tied to a particular camera (only available when the camera is selected). You access the *Event Buttons* window by clicking the *Event Buttons...* button in the *Administrator* window (see page 30).

Defined Events List

The *Event Buttons* window features a list of specified event buttons. When event buttons have been defined, you are able to expand elements in the list (by clicking ⊞) to get an overview of all defined event buttons; global event buttons as well as event buttons specified for individual cameras. Example:

Example: A global event button with an associated timer event has been specified. Also, two event buttons have been specified for an individual camera.

Specifying Event Buttons and Timer Events

To specify an event button, first determine whether you want the event button to be available globally or for a particular camera only.

Specifying Global Event Buttons

To specify a global event button, select the *Global* entry at the top of the *Defined Events* list, then click the *Add new event...* button. This will open the *Add New Event* window (for adding event buttons) – see page 98, in which you specify a name for the event button as well as whether the event button should trigger any e-mail or SMS alerts when clicked. When you click *OK* in the *Add New Event* window (for adding event buttons), you are returned to the *Event Buttons* window, in which your new event button will appear in the *Defined Events* list.

Specifying Camera-Specific Event Buttons

To specify an event button for a specific camera, select the required camera in the *Defined Events* list, then click the *Add new event...* button. This will open the *Add New Event* window (for adding event buttons) – see page 98, in which you specify a name for the event button as well as whether the event button should trigger any e-mail or SMS alerts when clicked. When you click *OK* in the *Add New Event* window (for adding event buttons), you are returned to the *Events* window (for specifying event buttons), in which your new event button will appear in the *Defined Events* list.

Specifying Timer Events

When you have specified an event button, you are able to associate timer events with the event button. Timer events are separate events, occurring a specified number of seconds or minutes after the event button has been clicked. Timer events may be used for a wide variety of purposes; the following are examples only:

- A camera starts when an event button is selected in the Smart Client (see page 175); a timer event stops the camera after 15 seconds
- A camera starts and the lights are switched on when an event button is selected in the Smart Client; a timer event stops the camera after one minute, and another timer event switches the lights off after two minutes

To define a timer event for an event button, select the required event button in he *Defined Events* list, then click the *Add new event...* button. When you click the *Add new event...* button while an already specified event button is selected in the *Defined Events* list, the *New Timer* window (see page 93) opens, allowing you to specify the required timer event.

Tip: You may specify several timer events under a single event button. However, you cannot use a timer event under another timer event.

Editing Event Buttons and Timer Events

To edit an event button, or a timer event specified under an event button, select the required event button or timer event in the *Defined Events* list, then click the *Edit selected...* button. If you have selected an event button, clicking the *Edit selected...* button will open the *Edit Event* window (for editing event buttons) – see page 99. If you have selected a timer event, clicking the *Edit selected...* button will open the *New Timer* window (see page 93).

Associating Event Buttons with External Outputs

As is the case with input events (see *External Input & Output* described on page 84), you are able to associate an event button with specific external outputs. This way, external output, for example the sounding of a siren, can be triggered automatically when an event button is clicked. Like with input, VMD and generic events, the association between event buttons and outputs is made in the *I/O Control* window (see page 105).

Add New Event Window (for Adding Event Buttons)

The *Add New Event* window (for adding event buttons) lets you specify the settings for an event button. You access the *Add New Event* window (for adding event buttons) from the *Event Buttons* window (see page 96): Select an entry (either *global* or for a specific camera) in the *Defined Events* list, then click the *Add new event...* button.

Add New Event Window's Fields

Field	Description
Button related to	Read-only field, displaying the name of the camera for which the event will be specified. If the field displays *Global*, the event button will be a global event button (available for all cameras).
Manual event name	Lets you specify a name for the event button. **Note:** Event button names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Send e-mail if this event occurs	Select check box to send an e-mail alert when the event button is clicked. In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 80).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the event button is

Field	Description
	clicked, in the e-mail alert, then select the required camera in the list below the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the event button is clicked. In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).

Edit Event Window (for Editing Event Buttons)

The *Edit Event* window (for editing event buttons) lets you edit the settings for an existing event button.

You access the *Edit Event* window (for editing event buttons) from the *Event Buttons* window (see page 96), by first selecting the required event button in the *Defined Events* list, then clicking the *Edit selected...* button.

Edit Event Window's Fields

The *Edit Event* window (for editing event buttons) contains the following fields:

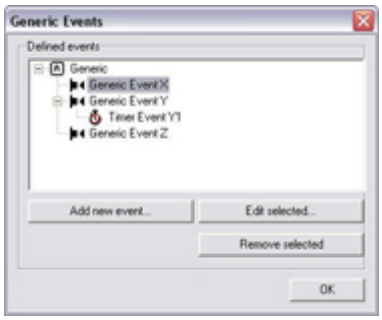
Field	Description
Button related to	Read-only field, displaying the name of the camera for which the event button has been specified. If the field displays *Global*, the event button is a global event button (available for all cameras).
Manual event name	Lets you edit the name of the event button. **Note:** Event button names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Send e-mail if this event occurs	Select check box to send an e-mail alert when the event button is clicked. In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 80).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the event button is clicked, in the e-mail alert, then select the required camera in the list below the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the event button is clicked. In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).

Generic Events

Generic Events Window

XProtect Enterprise is able to analyze received TCP and/or UDP data packages, and automatically trigger an event when specified criteria are met. This way you are able to easily integrate your XProtect Enterprise surveillance system with a very wide range of external sources, for example access control systems, alarm systems, etc.

Events based on the analysis of received TCP and/or UDP packets are called generic events. XProtect Enterprise listens for generic events on the port specified as *Alert Port* in the *Advanced* window – see page 95 (default is port 1234). The *Generic Events* window lets you manage such events.



You access the *Generic Events* window by clicking the *Generic Events* button in the *Administrator* window (see page 30).

Generic Events Window's Events List and Buttons

The *Generic E*vents window features a *Defined events* list, in which defined TCP- and/or UDP-based events are listed, as well a number of buttons used when configuring the events:

Button	Description
Add new event...	Lets you define new events. The type of event you are able to define is determined by what you have selected in the *Defined events* list: • When nothing is selected, or you have selected the list's *Generic* item, clicking the *Add new event...* button will open the *Add New Event* window (for specifying generic events) – see page 101, in which you are able to specify the rules and notification settings for individual TCP- and/or UDP-based events. • When an existing event is selected in the list, clicking the *Add new event...* button will open the *New Timer* window (see page 93), in which you are able to specify timer events. Timer events are separate events, triggered by the event under which they are defined. Timer events occur a specified number of seconds or minutes after the event under which they are defined has occurred.
Edit selected...	Opens the *Edit Event* window (for editing generic events) – see page 104 – in which you are able to edit the settings for an existing event selected in the *Defined events* list.
Remove selected	Lets you remove an existing event selected in the *Defined events* list. **Note:** The selected event will be removed without further warning.

Add New Event Window (for Specifying Generic Events)

The *Add New Event* window (for specifying generic events) lets you specify the settings for an event based on input from external sources using the TCP and UDP protocols: You are able to specify the criteria according to which XProtect Enterprise should analyze received TCP and/or UDP data packages, and whether any notifications should be triggered when the event occurs.

Tip: TCP and UDP packages used for generic events may contain special characters, such as @, #, +, å, ~, etc. within the text string to be analyzed.

You access the *Add New Event* window (for specifying generic events) from the *Generic Events* window (see page 100), by clicking the *Add new event...* button.

The *Add New Event* window (for specifying generic events) is divided into three sections:

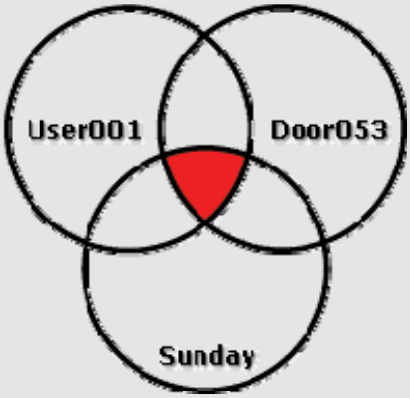
General Event Settings Section

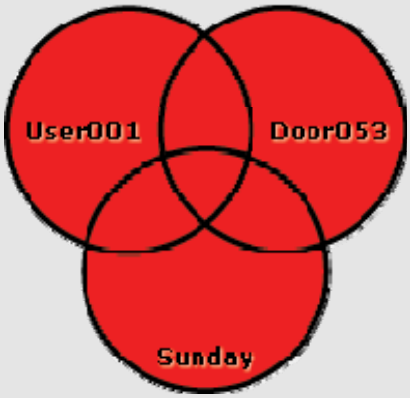
Field	Description
Event Name	Lets you specify a name for the event. Each event must have a unique name. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Event Protocol	Lets you select which protocol XProtect Enterprise should listen for in order to detect the event: • ***Any*:** Listen for, and analyze, packages using TCP as well as UDP protocol. • ***TCP*:** Listen for, and analyze, packages using TCP protocol only. • ***UDP*:** Listen for, and analyze, packages using UDP protocol only. **Which port is used?** XProtect Enterprise listens for generic events on the port specified as *Alert Port* in the *Advanced* window – see page 95 (default is port 1234).
Event rule type	Lets you select how particular XProtect Enterprise should be when analyzing received data packages: • ***Match*:** In order for the event to occur, the received package must contain *exactly* the message specified in the *Event rule string* section's *Event message include* field, and nothing else. • ***Search*:** In order for the event to occur, the received package must contain the message specified in the *Event rule string* section's *Event message include* field, but may also have more content. Example: If you have specified that the received package should contain the terms "User001" and "Door053", the event will be

Field	Description
	triggered if the received package contains the terms "User001" and "Door053" and "Sunday" as your required terms are contained in the received package.
Event priority	The same data package may be analyzed for different events. The ability to assign a priority to each event lets you manage which event should be triggered if a received package matches the criteria for several events. The priority must be specified as a number between 0 (lowest priority) and 1000 (highest priority). When XProtect Enterprise receives a TCP and/or UDP package, analysis of the packet will start with analysis for the event with the highest priority. This way, when a package matches the criteria for several events, only the event with the highest priority will be triggered. In case a package matches the criteria for several events with an identical priority, e.g. two events with a priority of *999*, all events with the priority in question will be triggered.

Event Rule String Section

Field, Button	Description
Event substring	Lets you specify the individual items for which XProtect Enterprise should look out when analyzing data packages. Specify one or more terms, then click the *Add* button to add the specified term(s) to the *Event message include* field, the content of which will be used for the actual analysis. Examples: • Single term: User001 (when added to the *Event message include* field, the term will appear as "User001") • Several terms as one item: User001 Door053 Sunday (when added to the *Event message include* field, the terms will appear as "User001 Door053 Sunday") When you add several terms as one item (appearing as e.g. "User001 Door053 Sunday" in the *Event message include* field), everything between the quotation marks must appear together in the package, in the specified sequence, in order to match your criterion. If the terms must appear in the package, but not necessarily in any exact sequence, add the terms one by one (i.e. so they will appear as "User001" "Door053" "Sunday" in the *Event message include* field).
Event message include	Displays the string which will be used for the actual package analysis. The field is not directly editable. However, you are able to position the cursor inside the field in order to determine where a new item should be included when you click the *Add* button or one of the parenthesis or operator buttons. Likewise, you are able to position the cursor inside the field in order to determine where an item should be removed when clicking the *Remove* button: The item immediately to the left of the cursor will be removed when you click the *Remove* button.

Field, Button	Description
Add	Adds the content of the *Event substring* field to the *Event message include* field, the content of which will be used for the actual analysis. See also the description of the *Event substring* and *Event message includes* fields.
(	Lets you add a start parenthesis character to the *Event message include* field. Parentheses can be used to ensure that related terms are processed together as a logical unit; in other words, they can be used to force a certain processing order in the analysis. Example: ("User001" OR "Door053") AND "Sunday" In the example, the two terms inside the parenthesis will be processed first, then the result will be combined with the last part of the string. In other words, the system will first look for any packages containing either of the terms *User001* or *Door053*, then it will take the results and run through them in order to see which packages also contain the term *Sunday*.
)	Lets you add an end parenthesis character to the *Event message include* field.
AND	Lets you add an AND operator to the *Event message include* field. With an AND operator you specify that the terms on both sides of the AND operator must be present. Example: User001 AND Door053 AND Sunday In the example, the term *User001* as well as the term *Door053* as well as the term *Sunday* must be present in order for the criterion to be met. It is *not* enough for only one or two of the terms to be present. As a rule of thumb, the more terms you combine with AND, the *fewer* results you will retrieve: 
OR	Lets you add an OR operator to the *Event message include* field. With an OR operator, you specify that either one or another term must be present. Example: User001 OR Door053 OR Sunday In the example, the term *User001* or the term *Door053* or the term *Sunday* must be present in order for the criterion to be met. The criterion is satisfied even if only one of the terms is present. As a rule of thumb, the more terms

Field, Button	Description
	you combine with OR, the *more* results you will retrieve: 
Remove	Lets you remove the item immediately to the left of a cursor positioned in the *Event message include* field. If no cursor has been positioned in the *Event message include* field, the last item in the field will be removed.

Notification Settings Section

Field	Description
Send Email if this event occurs	Select check box to send an e-mail alert when the event occurs. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 80).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the event is triggered, in the e-mail alert, then select the required camera in the list below the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the input occurs. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).

When you have specified a new generic event, click *OK*.

Edit Event Window (for Editing Generic Events)

The *Edit Event* window (for editing generic events) lets you edit the settings for an event based on input from external sources using the TCP and UDP protocols: You are able to edit the criteria according to which XProtect Enterprise should analyze received TCP and/or UDP data packages, and whether any notifications should be triggered when the event occurs.

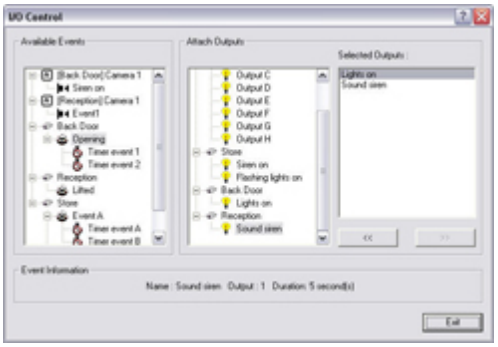
Tip: TCP and UDP packages used for generic events may contain special characters, such as @, #, +, å, ~, etc. within the text string to be analyzed.

You access the *Edit Event* window (for specifying generic events) from the *Generic Events* window (see page 100), by selecting an event from the list, then clicking the *Edit selected...* button.

See the description of the *Add New Event* window (for specifying generic events) on page 101 for further information.

Input/Output Control

I/O Control Window



In the *I/O Control* window you are able associate particular events and event buttons with one or more particular outputs. This way you are able to define that when a selected event occurs, or when a particular event button is clicked, one or more selected outputs will be triggered.

Note: Use of features in the *I/O Control* window requires that events and outputs have been specified (see *About Input, Events & Output ...* on page 84).

You access the *I/O Control* window from the *Administrator* window (see page 30), by clicking the *I/O Control...* button.

Associating Event with Particular Outputs

When associating an event with one or more outputs, you are able to select between **all** outputs defined on the XProtect Enterprise system; you are not limited to selecting outputs defined on a particular device.

To associate a particular event with a particular output, do the following:

1. Select the required event in the *Available Events* list in the left side of the *I/O Control* window.

   Tip: Events as well as event buttons may be listed. When you select an event or event button in the *Available Events* list, you can view detailed information about the selected event or event button under *Event Information* in the lower part of the window.

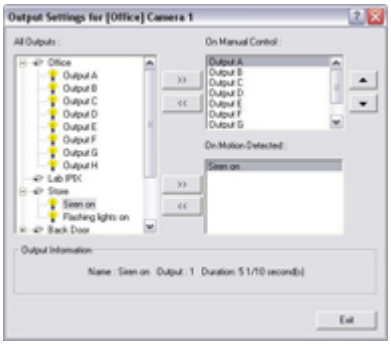
2. Select the required output in the list of available outputs (the list in the middle of the window).

3. Click the >> button located below the *Selected Outputs* list. This will copy the selected output to the *Selected Outputs* list. When the selected event occurs, or when the selected event button is clicked, the selected output will be triggered.

You are able to associate an event or an event button with more than one output: Simply repeat the process for each required output.

To remove an output from the *Selected Outputs* list, simply select the required output, and click the << button located below the *Selected Outputs* list.

Output Settings for [Device Name] [Camera Name] Window



In the *Output Settings for [Device Name] [Camera Name]* window you are able to associate a camera with particular external outputs, defined in the *I/O Setup* window (see page 86), for example the sounding of a siren or the switching on of lights. The associated outputs can be triggered automatically when motion is detected as well as manually through output buttons available in the Remote Client (see page 178) and Smart Client (see page 175).

You access the *Output Settings for [Device Name] [Camera Name]* window from the *Camera Settings for [Device Name] [Camera Name]* window (see page 43), by clicking the *Outputs...* button.

Associating Outputs with Manual Control and Detected Motion

Note: Use of features in the *Output Settings for [Device Name] [Camera Name]* window requires that output has been defined in the *I/O Setup* window (see page 86).

You have a high degree of flexibility when associating a camera with particular outputs:

- You are able to select between all available outputs, i.e. outputs defined as output events for the camera itself **as well as** outputs defined as output events for other devices on the XProtect Enterprise system
- The same output may be used for manual control through an output button **as well as** for automatic triggering when motion is detected

Selecting Output for Manual Control

You are able to specify outputs to be triggered manually from a list in the Remote Client (see page 178) or Smart Client (see page 175).

1. Select the required output in the *All Outputs* list in the left side of the *Output Settings for [Device Name] [Camera Name]* window. When you select an output in the *All Outputs* list, you can view detailed information about the selected output under *Output Information* in the lower part of the window.

2. Click the >> button located between the *All Outputs* list and the *On Manual Control* list. This will copy the selected output to the *On Manual Control* list. An unlimited number of outputs may be selected this way.

You are able to determine each output's position in the Remote Client's and Smart Client's output list by moving the selected output up or down in the *On Manual Control* list with the *up* and *down* buttons located to the right of the list. The selected output is moved up one step each time you click the *up* button. Likewise, each time you click the *down* button, the selected output is moved down one step.

To remove an output from the *On Manual Control* list, simply select the required output, and click the << button located between the *All Outputs* list and the *On Manual Control* list.

Selecting Output for Use on Motion Detection

You are able to select outputs to be triggered automatically when motion is detected in video from the camera. This feature does not require that a VMD (Video Motion Detection) event has been defined for the camera in the *I/O Setup* window (see page 86).

1. Select the required output in the *All Outputs* list in the left side of the *Output Settings for [Device Name] [Camera Name]* window.

   Tip: When you select an output in the *All Outputs* list, you can view detailed information about the selected output under *Output Information* in the lower part of the window.

2. Click the >> button located between the *All Outputs* list and the *On Motion Detected* list. This will copy the selected output to the *On Motion Detected* list.

To remove an output from the *On Motion Detected* list, simply select the required output, and click the << button located between the *All Outputs* list and the *On Motion Detected* list.

How to ...

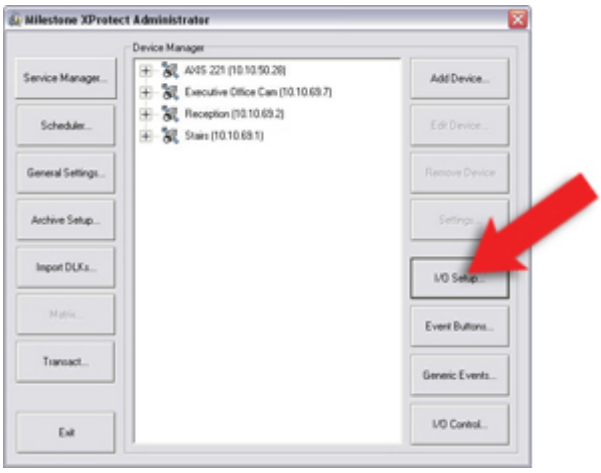
How to Add an Input-Based Event

Events can be used for automatically triggering actions in XProtect Enterprise, such as starting or stopping recording on cameras, triggering e-mail or SMS notifications, making PTZ cameras move to specific preset positions, activating output, etc.

Several types of events exist (see *About Input, Events & Output ...* on page 84). In the following you will see how to define events based on input received from external input units—such as sensors attached to doors, windows, etc.—connected to cameras or other devices on an XProtect Enterprise system.

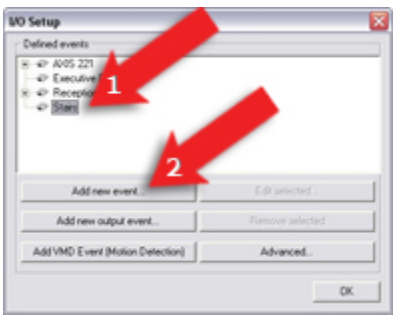
To add an input-based event, do the following:

1. In the *Administrator* window (see page 30), click the *I/O Setup* button.



   This will open the *I/O Setup* window (see page 86).

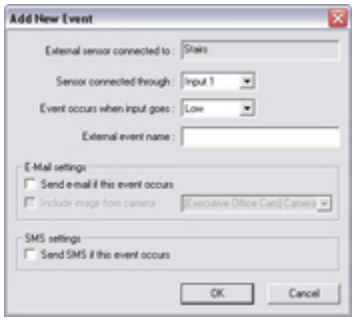
2. In the *I/O Setup* window, first select the camera or other device to which the input unit is connected, then click the *Add new event...* button. This will open the *Add New Event* window.



   Note: Some cameras/devices are capable of handling one input event only; others are capable of handling several input events. The content of the *Add New Event*

window varies accordingly. For simplicity reasons, the following steps will describe adding an event on a camera/device capable of handling one input event only.

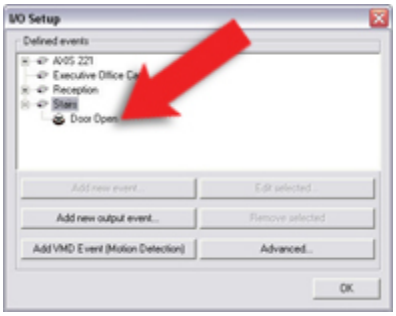
3. In the *Add New Event* window (for devices capable of handling one input event only), see page 88, the *External sensor connected to* field will show the name of the selected camera or other device. Now specify information in the following fields:



- *Sensor connected through*: Select the camera/device input port on which the input unit is connected. Some cameras/devices only have a single input port; in that case simply select *Input 1*.
- *Event occurs when input goes*: Select whether the input event should be triggered when the signal on the input sensor rises (*High*) or falls (*Low*).
- *External event name*: Specify a name for the event. Note that event names must *not* contain the following characters: < > & ' " \ / : * ? | [ ]
- (Optional) If requiring an e-mail alert to be sent automatically when the event occurs, select the *Send e-mail if this event occurs* check box. Note that in order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 80). If requiring an image (recorded at the time of the event) to be included in the e-mail alert, also check the *Include image from camera* check box and select the required camera in the list next to the check box.
- (Optional) If requiring an SMS mobile phone text message alert to be sent automatically when the event occurs, select the *Send SMS if this event occurs* check box. Note that in order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).

When ready, click *OK*. This will return you to the *I/O Setup* window (see page 86).

4. In the *I/O Setup* window, your newly defined event is now listed (you may have to click the expand icon ⊞ in front of the name of the camera or other device to see the listing):



Click *OK* to close the *I/O setup* window and return to the *Administrator* window (see page 30). For system administrators defining actions to be triggered by events, the event will now be selectable in line with other events defined on XProtect Enterprise.

How to Add an Event Button

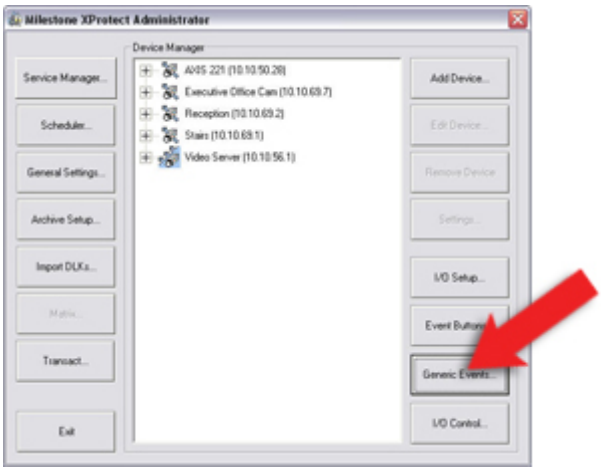
Events can be used for automatically triggering actions in XProtect Enterprise, such as starting or stopping recording on cameras, triggering e-mail or SMS notifications, making PTZ cameras move to specific preset positions, activating output, etc. An event may also trigger several actions simultaneously.

Several types of events exist (see *About Input, Events & Output* ...on page 84). In most cases, events occur and actions are triggered without the need for human intervention by XProtect Enterprise users: System administrators define the criteria for each event, for example a certain amount of detected motion or input from a specific sensor; when the criteria are met, the system interprets it as an event, and automatically triggers the required actions.

However, you may also want users to be able to manually force an event to occur. For this purpose, XProtect Enterprise lets you define event buttons. Event buttons let users manually trigger events from the Smart Client. In the Smart Client, event buttons are actually not buttons; instead users manually trigger events by selecting them from a list. See also 96 for examples of the many ways in which you can use event buttons.

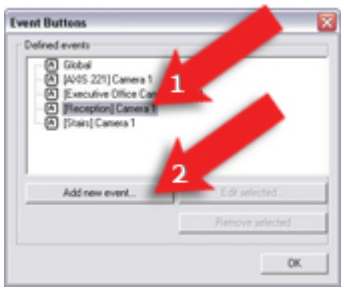
To add an event button, do the following:

1. In the *Administrator* window (see page 30), click the *Event Buttons...* button.



This will open the *Event Buttons* window (see page 96).

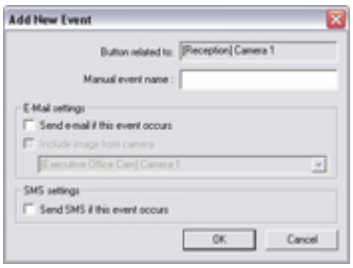
2. In the *Event Buttons* window, first select the camera or other device for which you want the event button to be available, then click the *Add new event...* button.



Note that you are also able to make the event button globally available (i.e. available to users regardless of which camera/device they have selected in the Smart Clients.

To make the event button globally available, simply select *Global* (at the top of the list) instead of a particular camera/device. This will open the *Add New Event* window (for adding event buttons) – see page 98.

3. In the *Add New Event* window (for adding event buttons), the *Button related to* field will show the name of the selected camera or other device. If you are adding a globally available event button, the field will display *Global*. Now specify information in the following fields:



   - *Manual event name*: Specify a name for the event button. Note that event names must *not* contain the following characters: < > & ' " \ / : * ? | [

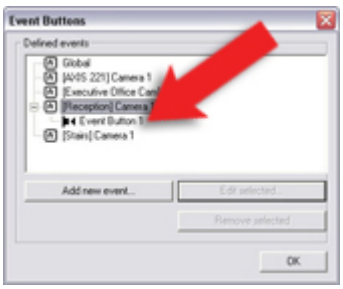
- (Optional) If requiring an e-mail alert to be sent automatically when the event occurs, select the *Send e-mail if this event occurs* check box. Note that in order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-*

Mail setup window (see page 80). If requiring an image (recorded at the time of the event) to be included in the e-mail alert, also check the *Include image from camera* check box and select the required camera in the list next to the check box.

- (Optional) If requiring an SMS mobile phone text message alert to be sent automatically when the event occurs, select the *Send SMS if this event occurs* check box. Note that in order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).

When ready, click *OK*. This will return you to the *Event buttons* window (see page 96).

4. In the *Event Buttons* window, your newly defined event button is now listed (you may have to click the expand icon ⊞ in front of the name of camera or other device to see the listing):



Click *OK* to close the *Event Buttons* window and return to the *Administrator* window (see page 30). The defined event button will now be available in the Smart Client (see page 175), as described in the beginning of this text. Note that individual users' rights may prevent them from accessing specific cameras and/or events in the Smart Client; such rights are defined through the *Image Server Administrator* window (see page 139). For system administrators defining actions to be triggered by events, the event button will now be selectable in line with other events defined on XProtect Enterprise.

How to Add a VMD Event

Events can be used for automatically triggering actions in XProtect Enterprise, such as starting or stopping recording on cameras, triggering e-mail or SMS notifications, making PTZ cameras move to specific preset positions, activating output, etc. An event may also trigger several actions simultaneously. Several types of events exist (see *About Input, Events & Output ...* on page 84). In the following, you will see how to define an event based on XProtect Enterprise detecting motion on a particular camera (VMD simply means Video Motion Detection). Once the VMD event is defined, you will be able to select it when further configuring XProtect Enterprise.

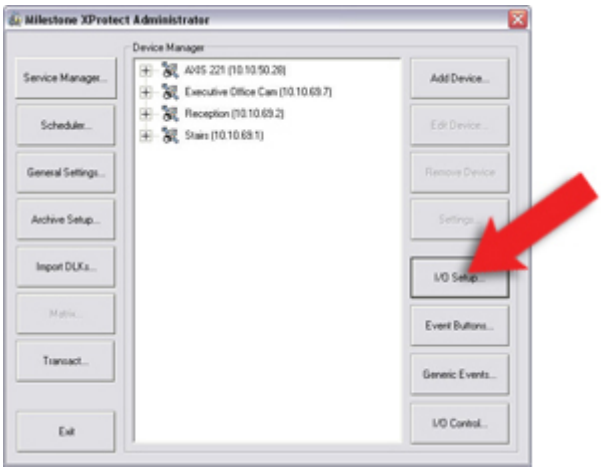
Tip: If you are specifically looking for information about how to configure motion detection-triggered activation of an output device only (such as a siren, a strobe light, etc.), see How to Add a Motion-Triggered Output on page 121.

Note: In addition to XProtect Enterprise's motion detection, some devices also have their own capabilities for detecting motion (configured in the devices' own software; typically by accessing a browser-based configuration interface on the device's IP address). Events based on motion detected *on a device itself* are not VMD Events; they are input events, since they are based on input from the device.

Note: Your motion detection settings for the camera in question will entirely determine when motion is detected, and thus when the VMD event will occur. See the description of the *Adjust Motion Detection* window (page 50) for more information. Also note that in order not to generate an excessively high number of VMD events during periods with lots of motion, a VMD event cannot occur more frequently than every five seconds.

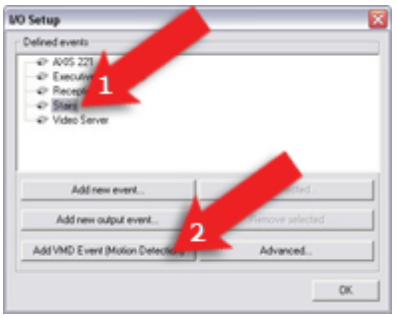
To add a VMD event, do the following:

1. In the *Administrator* window (see page 30), click the *I/O Setup* button.



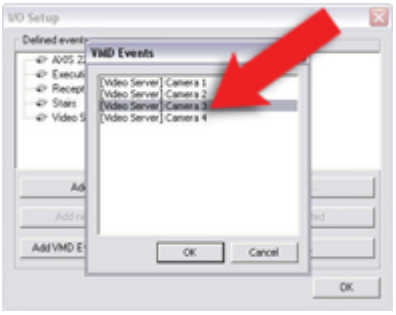
This will open the *I/O Setup* window (see page 86).

2. In the *I/O Setup* window, first select the device on which motion must be detected in order for the event to occur, then click the *Add VMD Event (Motion Detection)* button.

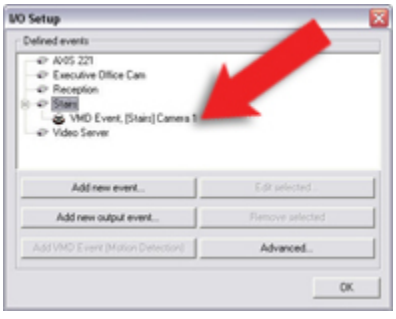


This will automatically add a VMD event to the selected device (unless the selected device is a video encoder, see below).

- If the selected device is a video encoder, several cameras may be attached to the device, and a separate dialog will prompt you to select the required camera:



3. In the *I/O Setup* window (see page 86), your newly defined VMD event will now be listed (you may have to click the expand icon ⊞ in front of the name of the device to see the listing):



Click *OK* to close the *I/O Setup* window (see page 86) and return to the *Administrator* window (see page 30). For system administrators defining actions to be triggered by events, the VMD event will now be selectable in line with other events defined on XProtect Enterprise.

Tip: For video encoder devices, you are able to define a VMD event for each connected camera; simply repeat above process.

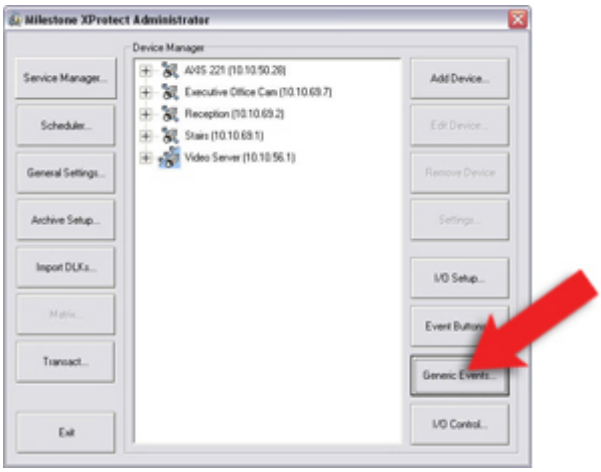
How to Add a Generic Event

XProtect Enterprise is able to analyze received TCP and/or UDP data packages, and automatically trigger an event when specified criteria are met. This way you are able to easily integrate your XProtect Enterprise surveillance system with a very wide range of external sources, for example access control systems, alarm systems, etc.

Events based on the analysis of received TCP and/or UDP packets are called generic events. XProtect Enterprise listens for generic events on the port specified as *Alert Port* in the *Advanced* window – see page 95 (default is port 1234).

To add a generic event, do the following:

1. In the *Administrator* window (see page 30), click the *Generic Events...* button.



This will open the *Generic Events* window (see page 100).

2. In the *Generic Events* window (see page 100), first select the *Generic* item, then click the *Add new event...* button:

This will open the *Add New Event* window (for specifying generic events) – see page 101.

3. Now specify information in the following fields:

- ***Event name*:** Specify a name for the event. Note that event names must *not* contain the following characters: < > & ' " \ / : * ? | [ ]

- ***Event Protocol*:** Select which protocol XProtect Enterprise should listen for: *Any* (i.e. TCP as well as UDP), *TCP* only, or *UDP* only. XProtect Enterprise listens for generic events on the port specified as *Alert Port* in the *Advanced* window – see page 95 (default is port 1234).

- ***Event rule type*:** Select how particular XProtect Enterprise should be when analyzing received data packages: *Match* if the received package must contain only the exact message specified in the *Event message include* field (see description in the following), *Search* if the received package must contain the message specified in the *Event message include* field, but may also have other content.

- ***Event priority*:** Specify a priority between 0 (lowest priority) and 1000 (highest priority) for the event, in case a received data package matches more than one event.

- ***Event rule string*:** Specify what XProtect Enterprise should look out for when analyzing the data packages, then click the *Add* button to add the specified term(s) to the *Event message include* field, the content of which is used when analyzing received data packages. You are furthermore able to use processing order parentheses and two different Boolean operators in the *Event message include* field by clicking the buttons to the right of the field.

- ***Send Email if this event occurs*:** (Optional) If requiring an e-mail alert to be sent automatically when the event occurs, select the *Send Email if this event occurs* check box. Note that in order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 80). If requiring an image (recorded at the time of the event) to be included in the e-mail alert, also check the Include image from camera check box and select the required camera in the list next to the check box.

- ***Send SMS if this event occurs*:** (Optional) If requiring an SMS mobile phone text message alert to be sent automatically when the event occurs, select the *Send SMS if this event occurs* check box. Note that in order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).

When ready, click *OK*. This will return you to the *Generic Events* window (see page 100).

4. In the *Generic Events* window, your newly defined event is now listed (you may have to click the expand icon ⊞ in front of the *Generic* item to see the listing):

Click *OK* to close the *Generic Event* window and return to the *Administrator* window (see page 30). For system administrators defining actions to be triggered by events, the generic event will now be selectable in line with other events defined on XProtect Enterprise.

Tip: See also How to Test a Generic Event below.

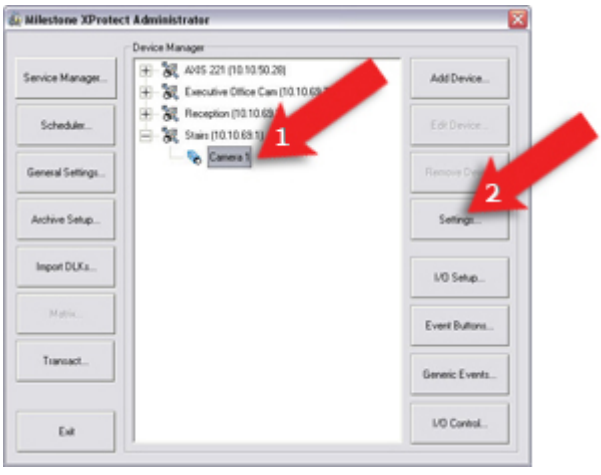
How to Test a Generic Event

Once you have added a generic event (see How to Add a Generic Event on page 112), a quick and easy way to test your generic event is to first set up an event notification and then use Telnet to send a small amount of data which will trigger the generic event and in turn the event notification.

What is Telnet? Telnet is a terminal emulation program used on TCP/IP networks. With Telnet, you can connect to a server from a computer on the network, and execute commands through Telnet as if you were entering them directly on the server. Windows includes a client for use with Telnet.

For this example, we have created a generic event called *Video*. Our generic event simply specifies that if the term *video* appears in a received TCP data package, the generic event should be triggered. Your generic event may be different, but you can still use the principles outlined in the following:

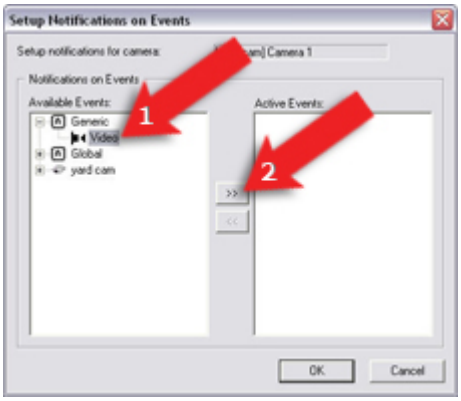
1. In the *Administrator* window (see page 30), first select a camera from which you are able to view video in a Remote Client/Smart Client, then click the *Settings* button:



This will open the *Camera Settings for [Device Name] [Camera Name]* window (see page 43).

2. In the *Camera Settings for [Device Name] [Camera Name]* window, click the *Event Notifications...* button: This will open the *Setup Notifications on Events* window (see page 54).

3. In the *Setup Notifications on Events* window's *Available Events* list, expand the *Generic* item and select your generic even Then click the >> button to move the selected generic event to the *Active Events* list:



Note: Make sure that your generic event is the *only* event appearing in the *Active Events* list while you are performing the test, otherwise you cannot be sure that it is your generic event which triggers the event notification. Once you are done testing, you can move any temporarily removed events back to the *Active Events* list.

4. Click *OK* in the *Setup Notifications on Events window*, click *OK* in the *Camera Settings for [Device Name] [Camera Name]* window (see page 43), then click the *Exit* button in the *Administrator* window (see page 30).

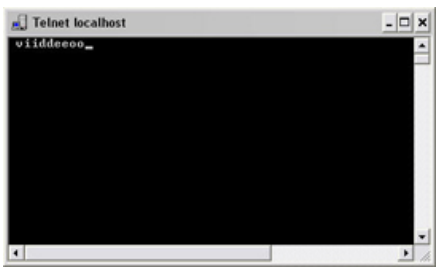
5. Make sure XProtect Enterprise's *Recording Server* service is running. Also make sure that the camera for which you configured the event notification is displayed in your Remote Client (see page 178) or Smart Client (see page 175).

6. In Windows' *Start* menu, select *Run...*, and type the following in the *Open* field:

   - **If you are performing the test on the XProtect Enterprise server itself:** `telnet localhost 1234`
   - **If you are performing the test from a remote computer:** Substitute *localhost* with the IP address of the XProtect Enterprise server. Example: If the IP address of the XProtect Enterprise server is 123.123.123.123, type: `telnet 123.123.123.123 1234`

Note: In the above examples, the number *1234* indicates the port on which the XProtect Enterprise server listens for generic events. Port 1234 is the default port for this purpose, but it is possible to change this by specifying another port number in the *Advanced* window's *Alert Port* field (see page 95). If the alert port number has been changed on your system, type your system's alert port number instead of *1234*.

This will open a *Telnet* window.



7. In the *Telnet* window, type the term (so-called *event substring*) required to trigger your generic event. In our case, the required term is *video*.

   While typing in the Telnet window, you may experience so-called echo. This is simply the server repeating some or all of the characters it receives; it

will not have any impact as long as you are sure you type the required characters.

8. Close the *Telnet* window by clicking the close button in its top right corner:

9. Go to your Remote Client (see page 178) or Smart Client (see page 175). If the yellow event notification indicator lights up for the required camera, your generic event works as intended:

How to Add a Timer Event

Timer events are separate events, triggered by the input event, VMD event, generic event or event button under which they are defined. Timer events occur a specified number of seconds or minutes after the event under which they are defined has occurred or the event button under which they have been defined has been clicked.

Timer events may be used for a wide variety of purposes; the following are examples only:

- A camera starts recording based on an input event, e.g. when a door is opened; a timer event stops the recording after 15 seconds

- Lights are switched on and a camera starts recording based on a VMD event, i.e. when motion is detected; a timer event stops the recording after one minute, and another timer event switches the lights off after two minutes

To define a timer event, do the following:

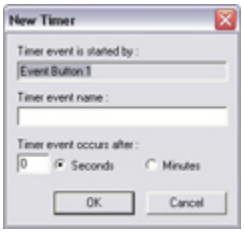
1. A timer event requires that an input event, VMD event, generic event or event button has already been defined. Begin by selecting the required event or event button:

    - **If Adding the Timer Event under an Already Defined Input or VMD Event:** Click the *Administrator* window's (see page 30) *I/O Setup...* button to open the *I/O Setup* window (see page 86): In the *I/O Setup* window's *Defined events* list, click the plus sign (⊞) next to the required device, select the required input or VMD event, then click the *Add new event...* button to open the *New Timer* window (see page 93).

    - **If Adding the Timer Event under an Already Defined Event Button:** Click the *Administrator* window's (see page 30) *Event Buttons...* button to open the *Event Buttons* window (see page 96): In the *Event Buttons* window's *Defined Events* list, select the required event button, then click the *Add new event...* button to open the *New Timer* window.

- **If Adding the Timer Event under an Already Defined Generic Event:** Click the *Administrator* window's (see page 30) *Generic Events...* button to open the *Generic Events* window (see page 100): In the *Generic Events* window's *Defined Events* list, select the required generic event, then click the *Add new event...* button to open the *New Timer* window.

2. In the *New Timer* window (see page 93), the *Timer event is started by* field will show the name of the selected event or event button. Now specify information in the following fields:

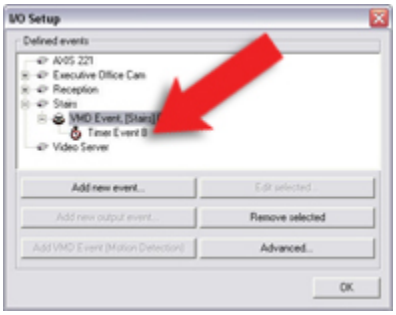


   - ***Timer event name*:** Specify a name for the timer event. Note that event names must *not* contain the following characters: < > & ' " \ / : * ? | [ ]

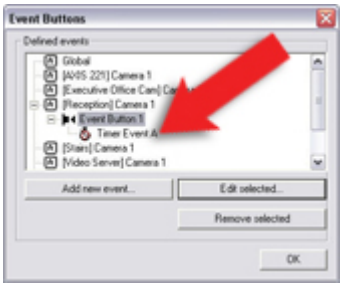
   - ***Timer event occurs after*:** Specify the amount of time that should pass between the event occurring/event button being clicked and the timer event, in either seconds or minutes.

   When ready, click *OK*.

3. In the window from which you opened the *New Timer* window (see page 93), your newly defined timer event will now be listed:



Timer event (in this example associated with a VMD event) listed in I/O Setup window (see page 86). You may have to click the expand icon ⊞ in front of the name of the required device as well as the required main event to see the timer event.



Timer event (associated with an event button) listed in Event Buttons window (see page 96). You may have to click the expand icon ⊞ in front of the name of the required device as well as the required main event to see the timer event.

Timer event (associated with a generic event) listed in Generic Events window (see page 100). You may have to click the expand icon ⊞ in front of the word Generic as well as the required main event to see the timer event.

Click *OK* to return to the *Administrator* window (see page 30).

For system administrators defining actions to be triggered by events, the timer event will now be selectable in line with other events defined on XProtect Enterprise.

How to Add a Manually Controlled Output

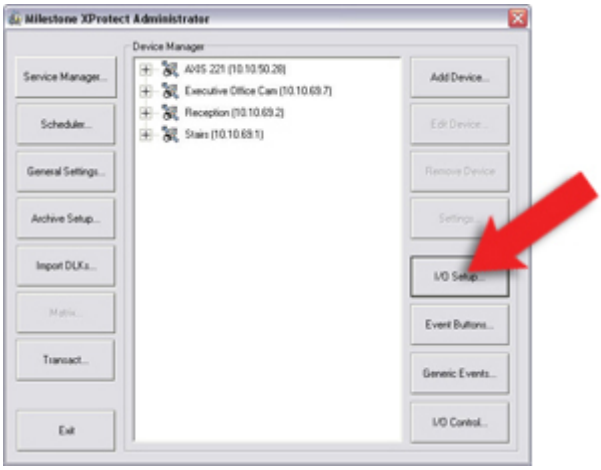
Output (e.g. lights, sirens, etc.) connected to cameras or other devices can be triggered manually when viewing live video in the Remote Client (see page 178) and Smart Client (see page 175). In the Remote Client and Smart Client, the output is triggered by selecting the required output from a list on the client's *Live* tab.

The output does not necessarily have to be physically connected to the specific camera from which a Remote Client /Smart Client user views live video; the output can be connected to any device on your XProtect Enterprise system.

To add an output for manual control, do the following:

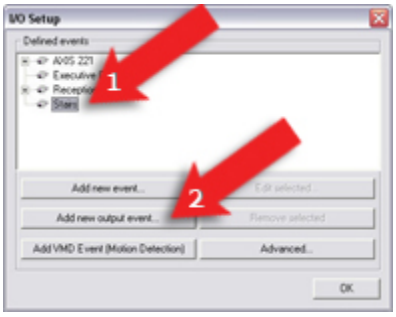
Note: In the following, it is assumed that the required output unit has been connected to the output port on the required camera or other device, but that it has not yet been defined on your XProtect Enterprise system. If you have already defined the output on your system, begin at step 5.

1. In the *Administrator* window (see page 30), click the *I/O Setup* button.



   This will open the *I/O Setup* window (see page 86).

2. In the *I/O Setup* window, first select the camera or other device to which the output unit is connected, then click the *Add new output event...* button:



   This will open the *Add New Output* window (see page 94).

3. In the *Add New Output* window, the *External output connected to* field will show the name of the selected camera or other device. Now specify information in the following fields:

   - ***Output connected on*:** Select the camera/device output port on which the output unit is connected. Many cameras/devices only have a single output port; in that

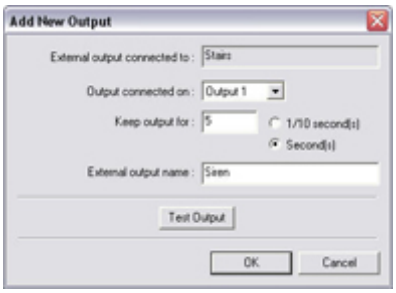
case simply select *Output 1*.

- ***Keep output for*:** Specify the amount of time for which the output should be active when triggered, in either 1/10 seconds or seconds.

  Note: Some devices are only able to apply outputs for a relatively short time, for example max. five seconds. Refer to the documentation for the device in question for exact information.

- ***External output name*:** Specify a name for the output. The name will appear on the list with which users will be able to manually trigger the output. Note that output names must *not* contain the following characters: < > & ' " \ / : * ? | [ ]

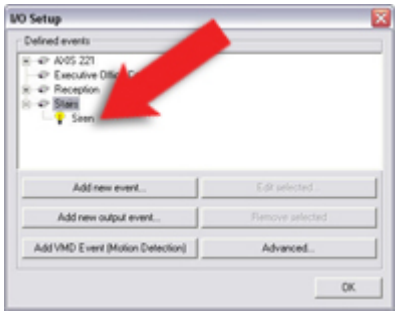
In the example to the right, we have specified that a siren connected on a camera's Output 1 port should sound for five seconds when triggered:



Tip: You are able to test the output by clicking the *Test Output* button.

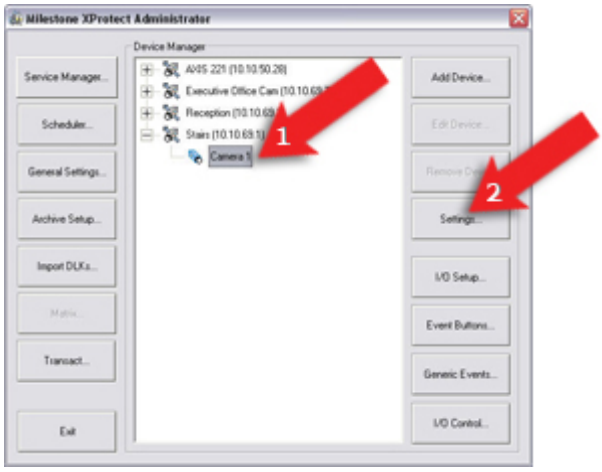
When ready, click *OK*. This will return you to the *I/O Setup* window (see page 86).

4. In the *I/O Setup* window, your newly defined output is now listed (you may have to click the expand icon ⊞ in front of the name of the camera or other device to see the listing):



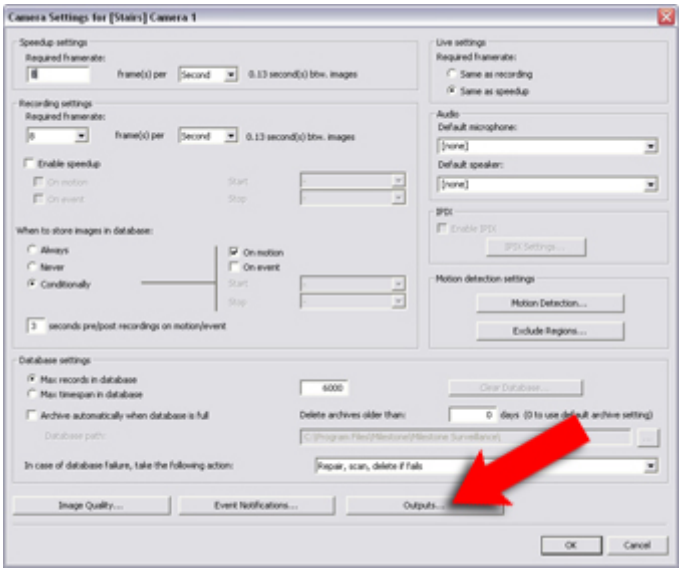
Click *OK* to close the *I/O setup* window and return to the *Administrator* window (see page 30).

5. In the *Administrator* window (see page 30), first select the camera for which the output should be available, then click the *Settings...* button.



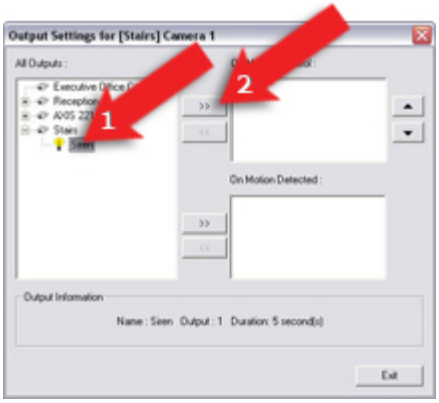
This will open the *Camera Settings for [Device Name] [Camera Name]* window (see page 43).

6. In the *Camera Settings for [Device Name] [Camera Name]* window, click the *Outputs...* button:



This will open the *Output Settings for [Device Name] [Camera Name]* window (see page 106).

7. In the *All Outputs* list in the window's left side, select the required output, then click the >> button located between the *All Outputs* list and the *On Manual Control* list:



This will copy the selected output to the *On Manual Control* list, which lists all outputs available for manual control when viewing live video from the camera in question.

Good to know:

- You are not limited to selecting output connected to the camera itself. If output has been defined on other cameras/devices on the XProtect Enterprise system, this output will also be selectable in the *All Outputs* list.
- An unlimited number of outputs may be selected this way.
- If you have specified several outputs in the *On Manual Control* list, you are able to control the sequence in which the outputs will be displayed in the Remote Client (see page 178) and Smart Client (see page 175). By using the *up* and *down*

buttons located to the right of the list, you can change a selected output's position in the sequence.

- The *Output Settings for [Device Name] [Camera Name]* window (see page 106) also lets you select output for automatic triggering on detected motion. This is further described in How to Add a Motion-Triggered Output on page 121.

8. When ready, click the *Output Settings for [Device Name] [Camera Name]* window's *Exit* button to return to the *Camera Settings for [Device Name] [Camera Name]* window (see page 43).

9. In the *Camera Settings for [Device Name] [Camera Name]* window, click *OK* to return to the *Administrator* window (see page 30).

10. Close the *Administrator*. The defined output will now be available in the Remote Client Client/Smart Client, as described in the beginning of this text. Note that individual users' rights may prevent them from accessing specific cameras and/or output in the Remote Client and Smart Client; such rights are defined through the *Image Server Administrator* window (see page 139).

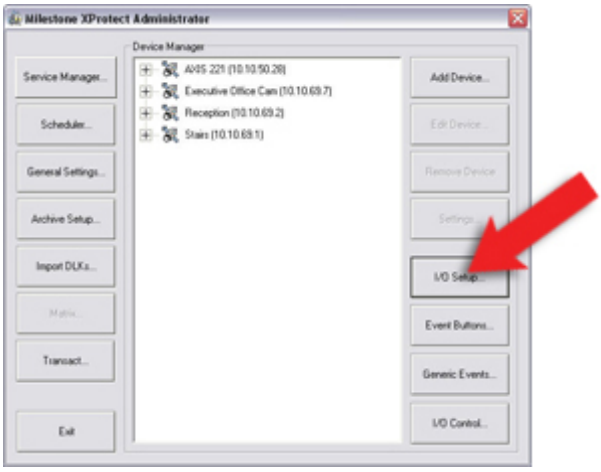
How to Add a Motion-Triggered Output

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

Output (e.g. lights, sirens, etc.) connected to cameras or other devices can be triggered automatically when motion is detected by a camera. The output does not necessarily have to be physically connected to the motion-detecting camera.

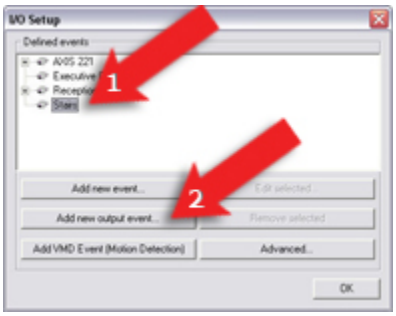
Note: The following describes *one* way of adding a motion-triggered output, namely through the *Output Settings for [Device Name] [Camera Name]* window (see page 106). Alternatively, motion-triggered output may be based on VMD events or—if a device has its own motion detection capabilities—on input events. Once such VMD or input events have been added, they can be tied to output through the *I/O Control* window (see page 105). In the following, it is assumed that the required output unit has been connected to the output port on the required camera or other device, but that it has not yet been defined on your XProtect Enterprise system. If you have already defined the output on your system, begin at step 5.

1. In the *Administrator* window (see page 30), click the *I/O Setup* button.



This will open the *I/O Setup* window (see page 86).

2. In the *I/O Setup* window (see page 86), first select the camera or other device to which the output unit is connected, then click the *Add new output event...* button:



This will open the *Add New Output* window 94.

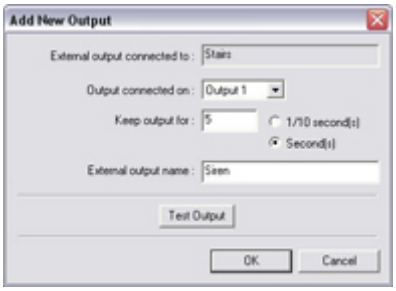
3. In the *Add New Output* window, the *External output connected to* field will show the name of the selected camera or other device. Now specify information in the following fields:

- ***Output connected on*:** Select the camera/device output port on which the output unit is connected. Many cameras/devices only have a single output port; in that case simply select *Output 1*.
- ***Keep output for*:** Specify the amount of time for which the output should be active when triggered, in either 1/10 seconds or seconds.

  Note: Some devices are only able to apply outputs for a relatively short time, for example max. five seconds. Refer to the documentation for the device in question for exact information.

- ***External output name*:** Specify a name for the output. The name will appear on the list with which users will be able to manually trigger the output. Note that output names must *not* contain the following characters: < > & ' " \ / : * ? | [ ]

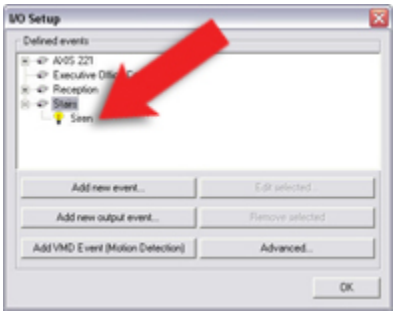
In the example to the right, we have specified that a siren connected on a camera's Output 1 port should sound for five seconds when triggered:



Tip: You are able to test the output by clicking the *Test Output* button.

When ready, click *OK*. This will return you to the *I/O Setup* window (see page 86).

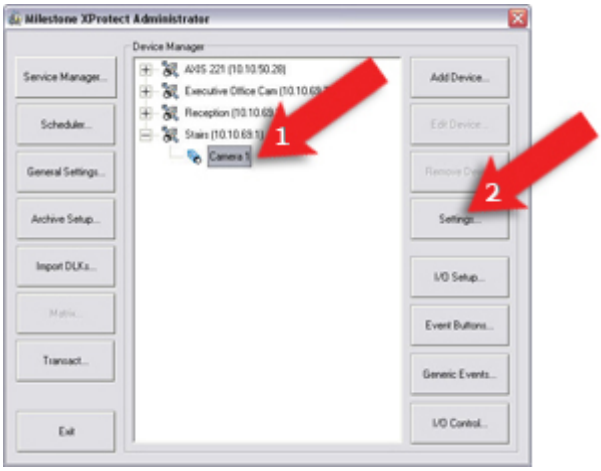
4. In the *I/O Setup* window, your newly defined output is now listed (you may have to click the expand icon ⊞ in front of the name of the camera or other device to see the listing):



Click *OK* to close the *I/O setup* window (see page 86) and return to the *Administrator*

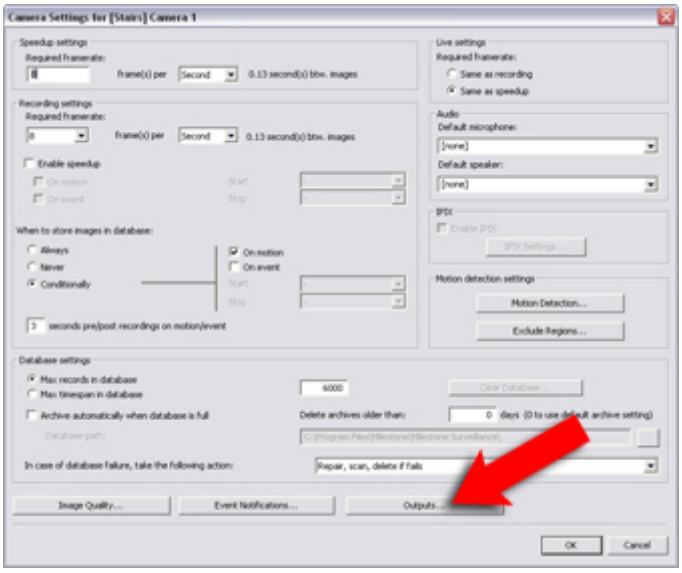
window (see page 30).

5. In the *Administrator* window (see page 30), first select the camera for which the output should be available, then click the *Settings...* button.



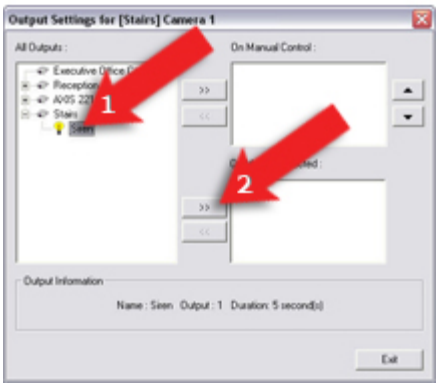
This will open the *Camera Settings for [Device Name] [Camera Name]* window (see page 43).

6. In the *Camera Settings for [Device Name] [Camera Name]* window, click the *Outputs...* button:



This will open the *Output Settings for [Device Name] [Camera Name]* window (see page 106).

7. In the *All Outputs* list in the window's left side, select the required output, then click the >> button located between the *All Outputs* list and the *On Motion Detected* list:



This will copy the selected output to the *On Motion Detected* list, which lists all outputs to be automatically triggered when motion is detected by the camera.

Good to know:

- You are not limited to selecting output connected to the camera itself. If output has been defined on other cameras/devices on the XProtect Enterprise system, this output will also be selectable in the *All Outputs* list.
- An unlimited number of outputs may be selected this way.
- The *Output Settings for [Device Name] [Camera Name]* window also lets you select output for manual triggering in the Remote Client and Smart Client. This is further described in How to Add a Manually Controlled Output on page 118.

8. When ready, click the *Output Settings for [Device Name] [Camera Name]* window's *Exit* button to return to the *Camera Settings for [Device Name] [Camera Name]* window.

9. In the *Camera Settings for [Device Name] [Camera Name]* window, click *OK* to return to the *Administrator* window.

10. Close the *Administrator*. The defined output will now be triggered automatically when motion is detected by the selected camera. Note that the automatic output triggering will be controlled entirely by your motion detection settings for the camera in question. See the description of the *Adjust Motion Detection* window (page 50) for more information.

Archiving

With the daily archiving feature in XProtect Enterprise, you are able to keep recordings for as long as required, limited only by the available hardware storage capacity.

You enable and configure archiving in the *Archive setup* window (see page 130). The *Archive setup* window also lets you specify where archives should be stored for each camera.

Benefits of Archiving

By default, information received from cameras is stored by XProtect Enterprise in a database for each camera.

The database for each camera (see *Camera Settings for [Device Name] [Camera Name]* window described on page 43) is capable of containing a maximum of 600,000 records or 40 GB before the oldest records in the database are overwritten.

With daily archiving, the amount of records you are able to store is limited only by the available hardware storage capacity.

By using archiving, you will also be able to back up archived records on backup media of your choice, using your preferred backup software.

How Archiving Works

For each camera, for which archiving has been specified, the contents of the camera database will be moved to a default archiving directory called *Archives*. This will happen automatically one or more times every day, depending on your archiving settings.

The default archiving directory is located on the computer running the XProtect Enterprise software, by default in the directory containing the XProtect Enterprise software (typically c:\program files\milestone\milestone surveillance\archives\).

In the archiving directory, separate sub-directories for storing archives for each camera are automatically created. These sub-directories are named after the MAC address of the device to which the camera is connected.

Since you are able to keep archives spanning many days of recordings, and since archiving may take place several times a day, further sub-directories, named after the archiving date and time, are also automatically created.

The sub-directories will be named according to the following structure:

```
...\Archives\CameraMACAddress_VideoEncoderChannel\DateAndTime
```

Example: With the default archiving folder located under C:\MyFiles\MySurveillanceSystem, video from an archiving taking place at 23.15 on 1st June 2005 for a camera attached to channel 2 on a video encoder device with the MAC address 00408c51e181 would be stored at the following destination:

```
C:\MyFiles\MySurveillanceSystem\Archives\00408c51e181_2\2005-06-01-23-15
```

If the device to which the camera is attached is not a video encoder device with several channels, the video encoder channel indication in the sub-directory named after the device's MAC address will always be *_1*. Example: (e.g. 00408c51e181_1)

Storing Archives at Other Locations than the Default Archiving Directory

You are of course also able to store archives at other locations than locally in the default archiving directory. You may, for example, specify that your archives should be stored on a network drive.

When archiving to other locations than the default archiving directory, XProtect Enterprise will first store the archive in the local default archiving directory, then immediately move the archive to the archiving location you have specified.

While this may at first glance seem unnecessary, it greatly speeds up the archiving procedure, which will reduce delays in case of network problems.

Archiving directly to a network drive would mean that archiving time would vary depending on the available bandwidth on the network. First storing the archive locally, then moving it, ensures that the archiving is always performed as fast as possible.

If archiving to a network drive, note the regular camera database **must** still be stored on a local drive, i.e. a drive attached directly to the computer running the XProtect Enterprise system.

Archiving Audio

If audio is enabled on a device, audio from the device will also be archived. If the device is a video encoder with several channels, audio will be archived with the camera on channel 1.

When an audio source is enabled, audio is recorded to the associated camera's database. This will affect the database's capacity for storing video. It is thus important to bear in mind that the maximum limit of the database is likely to be reached earlier if recording audio *and* video than if only recording video.

You may thus want to archive more frequently if recording audio *and* video than if only recording video.

Storage Capacity Required for Archiving

The storage capacity required for archiving depends entirely on the amount of recordings you plan to archive.

Some organizations want to keep archived recordings from a large number of cameras for several months or years. Other organizations may only want to archive recordings from one or two cameras, and they may want to keep their archives for much shorter periods of time.
Before enabling archiving, you should always consider the storage capacity of the **local** drive containing the default archiving directory to which archives are always moved, even though they may immediately after be moved to an archiving location on a network drive: As a rule of thumb, the capacity of the local drive should be at least twice the size required for storing the databases of all cameras for which archiving has been specified.

When archiving data from a camera to **external** locations, including archiving locations on network drives, XProtect Enterprise automatically checks that the space required for data to be archived *plus* 1 GB of free disk space is available at the external location. If not, the external archive location's oldest data from the camera in question will be deleted until there is sufficient free space for the new data to be archived.

In short: When estimating storage capacity required for archiving, consider your organization's needs, then plan for worst case rather than best case scenarios.

Tip: Milestone's server estimator and storage calculator features, found in the *Support* section of the Milestone website, www.milestonesys.com, can help you easily determine the capacity required for your surveillance system.

Automatic Response if Running Out of Disk Space

With archiving, XProtect Enterprise can automatically respond to the threat of running out of disk space. Two scenarios can occur, depending on whether the camera database drive is different from, or identical to, the archiving drive:

Different Drives: Automatic Archiving if Database Drive Runs Out of Disk Space

In case the XProtect Enterprise server is running out of disk space, and

- the archiving drive is ***different from*** the camera database drive, and
- archiving has not taken place within the last hour,

archiving will automatically begin in an attempt to free up disk space. This will happen regardless of any archiving schedules, but will of course only apply for cameras for which archiving has been enabled in the *Archive Setup* window (see page 130).

The server is considered to be running out of disk space if:

- there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera

  - or -

- the available disk space goes below 150 MB plus 20 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras))

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

On the archiving drive, XProtect Enterprise automatically checks that the space required for data from a camera to be archived plus 1 GB of free disk space per camera is available. If not, the archive drive's oldest data from the camera in question will be deleted until there is sufficient free space for the new data to be archived.

IMPORTANT: You will lose the archive data being deleted.

Same Drive: Automatic Moving or Deletion of Archives if Running Out of Disk Space

In case the XProtect Enterprise server is running out of disk space, and the archiving drive is ***identical to*** the camera database drive, XProtect Enterprise will automatically do the following in an attempt to free up disk space:

1. First, XProtect Enterprise will attempt to move archives (moving archives is only possible if you use dynamic archiving, with which you can archive to several different drives; see page 134). This will happen if:
   - there is less than 15% disk space left, and the available disk space goes below 40 GB plus 2 GB per camera

     - or –

- the available disk space goes below 225 MB plus 30 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 525 MB (225 MB plus 30 MB for each of the ten cameras))

The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 15% disk space left.

2. If moving archives is not possible, XProtect Enterprise will attempt to delete the oldest archives. This will happen if:
   - there is less than 10% disk space left, and the available disk space goes below 30 GB plus 1.5 GB per camera

     - or -
   - the available disk space goes below 150 MB plus 20 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 350 MB (150 MB plus 20 MB for each of the ten cameras))

   The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

   IMPORTANT: You will lose data from the archives being deleted.

3. Ultimately, if there are no archives to delete, XProtect Enterprise will attempt to resize camera databases by deleting their oldest recordings. This will happen if:
   - there is less than 5% disk space left, and the available disk space goes below 20 GB plus 1 GB per camera

     - or -
   - the available disk space goes below 75 MB plus 10 MB per camera (example: with ten cameras, the server would be running out of disk space if the remaining available disk space went below 175 MB (75 MB plus 10 MB for each of the ten cameras))

   The difference ensures that very large disks will not necessarily be considered to be running out of disk space just because they have less than 10% disk space left.

   IMPORTANT: You will lose data from the archives being deleted.

   When the recording server is restarted upon such database resizing, the original database sizes will be used. You should therefore make sure the drive size problem is solved, or adjust camera database sizes to reflect the altered drive size.

   Tip: Should the database resizing procedure take place, you will be informed on-screen in the Smart Client, in log files, and (if set up) through an e-mail and/or SMS alert.

Backing Up Archives

Many organizations want to back up recordings from cameras, using tape drives or similar. Creating such backups based on the content of camera databases is not recommended; it may cause sharing violations or other malfunctions.

Instead, create such backups based on the content of archives. If you have not specified separate archiving locations for separate cameras, you could simply back up the default local archiving directory, *Archives*.

When scheduling a backup, make sure the backup job does not overlap with your specified archiving times.

Viewing Archived Recordings

You view archived recordings in the Viewer (see page 169) or *Smart Client* (see page 175). This way, you are able to use all of *Viewer*'s or *Smart Client*'s advanced features (video browsing, smart search, evidence generation, etc.) for archived recordings as well.

Archives Stored Locally or on Network Drives

For archived recordings stored locally or on network drives you simply use the *Viewer*'s or *Smart Client*'s browsing features, for example the timeline browser or the playback controls, for finding and viewing the required recordings; just like you would with recordings stored in a camera's regular database.

Exported Archives

For exported archives, e.g. archives stored on a CD, you must use the *Viewer*: Click the browse button in the *Viewer*'s *Database Information* control panel to browse for the archive you want to view. Once you have specified the required archive this way, you can use all of the *Viewer*'s browsing features for navigating the recordings in the archive. See also the separate Milestone XProtect Viewer manual.

Virus Scanning and Archiving

If allowed in your organization, disable any virus scanning of camera databases and archiving locations. For more information see Virus Scanning Information on page 162.

New Database if Archiving Fails

Under extremely rare circumstances archiving may fail. For example, a database may be full and ready for archiving, but the operating system may lock content in the database if a content file is open. This would prevent archiving. In practice, this situation would only occur if somebody attempted to view a database file (e.g. a .pic file) directly from the database folder at the time of the archiving (viewing the file directly would not work since database content cannot be viewed as individual files, only through a Smart Client or Viewer).

In such situations, the database will be put aside for archiving at a later point in time. While the database is put aside, a special temporary database is created for storage of new recordings. This way, no new recordings will be lost even though the original database is full (provided enough disk space is available for storing the special temporary database).

XProtect Enterprise will wait for the next archiving occasion (either scheduled or because the special temporary database also becomes full). It will then archive the content of the special temporary database, and thus free up space in it. XProtect Enterprise will then continue to store new recordings in the special temporary database. This will apply until the Recording Server service is restarted (see page 68). Once the service has been restarted, the content of the original database will be archived, and new recordings will again be stored in the original database. The special temporary database will also be archived, and will then cease to exist.

Can I view recordings from the special temporary database? Normally, the content of databases can be viewed through a Smart Client or Viewer, regardless whether the databases have been archived or not. However, the content of the special temporary database cannot be viewed through a Smart Client until the content has been archived. On the surveillance server itself, you will be able to view the content of the special temporary database through the Viewer, even if the special temporary database has not been archived yet.

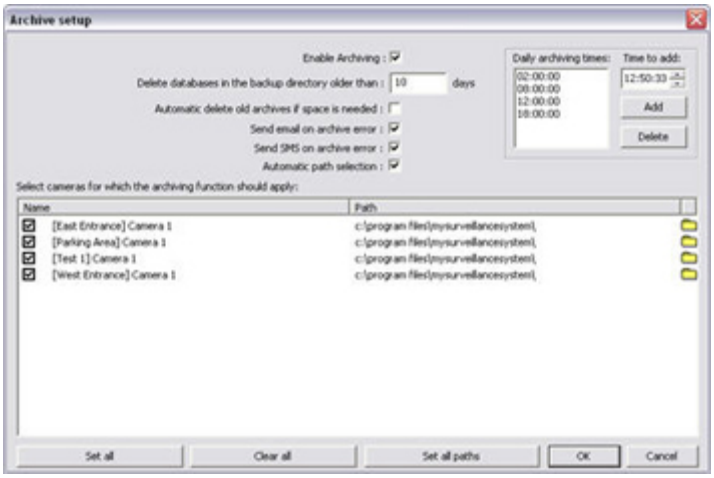
Since the special temporary database will be used for storing new recordings until the Recording Server service is restarted—even though the original database may no longer be locked—you may

in these extremely rare situations experience that new recordings are not viewable through Smart Clients. In that case, restarting the Recording Server service will help, since it will force the original database to again be used for storing new recordings.

Archive Setup Window

The *Archive setup* window lets you enable and configure the archiving feature in XProtect Enterprise. It also lets you specify where archives should be stored for the cameras.

To access the *Archive setup* window, click the *Archive Setup...* button in the *Administrator* window (see page 30).



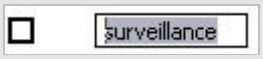
Archive Setup Window's Fields and Buttons

The *Archive setup* window contains the following fields and buttons:

Field, Button	Description
Enable Archiving	Select check box to enable the archiving feature. **Note:** Remember to specify for which cameras the archiving feature should be used; you do this in the *Select cameras for which the archiving function should apply* section at the bottom of the window.
Delete databases in the backup directory older than	Lets you specify how many days you want to keep archived recordings for. Archived recordings older than the specified number of days will automatically be deleted. In the Camera Settings for [Device Name] [Camera Name] window (see page 43) you can overwrite this setting for a specific camera.
Automatically delete old archives if space is needed	**Note:** You can only change this option if the *Automatic path selection* check box (see below) is also selected. If the *Automatic path selection* check box is not selected, automatic deletion of old archives will always be active. If you select this check box, the oldest archives will automatically be deleted until there is enough space when new recordings are moved to the archives. If you do not select this check box, and the archives are full, your recordings will remain in the local database. When the local database runs out of space, the oldest recordings will be deleted.
Send email on archive error	Select check box if XProtect Enterprise should send an e-mail alert if archiving fails, for example because the disk is full. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must

Field, Button	Description
	have been set up in the *E-Mail setup* window (see page 80).
Send SMS on archive error	Select check box if XProtect Enterprise should send an SMS (mobile phone text message) alert if archiving fails, for example because the disk is full. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 82).
Automatic path selection	Lets you select locations for archiving for all cameras in one go. This will divide the bottom of the window into two sections: *Select cameras for which the archiving function should apply* and *Select drives for dynamic archives.* See descriptions in the following.
Daily archiving times	Lists specified archiving times. Archiving will take place every day at the specified times. Archiving once a day will normally suffice. However, if you expect the daily database per camera to exceed 40 GB or 600,000 records, you should specify additional archiving times. To add an archiving time to the list, specify the required time in the *Time to add* field, then click the *Add* button. There must be at least one hour between each archiving time. To remove an archiving time from the list, select the archiving time to remove from the list, and click the *Delete* button. **Note:** While archiving takes place, cameras for which archiving applies will briefly stop recording, one after the other. Although the pause is very brief (typically less than a second), it is therefore recommended that you specify archiving times that are outside periods in which you expect to record important video.
Time to add	Lets you add an archiving time to the *Daily archiving times* list. You specify the required time by selecting the hour, minute and second values respectively, then clicking the field's *up* and *down* buttons to increase or decrease values. **Tip:** You may also simply overwrite selected hour, minute or second values.
Add	Adds the archiving time specified in the *Time to add* field to the *Daily archiving times* list.
Delete	Removes a selected archiving time from the *Daily archiving times* list.
Select cameras for which the archiving function should apply	If the *Archive Setup* window's *Enable Archiving* check box is selected, this section lists cameras for which archiving is possible. The section lists all enabled cameras, i.e. cameras which, depending on their individual settings, may transfer video to the surveillance system. The section also lists the path to the archiving directory for each camera. **Tip:** If a particular camera is not listed, it is highly likely that the camera is disabled. To check if a camera is disabled, look for the camera in the

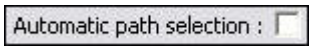
Field, Button	Description
	Administrator window's (see page 30) *Device Manager* section. A disabled camera will be clearly indicated by an icon, and can be enabled if you right-click the camera name. **Specifying that Archiving Should Apply for Specific Cameras** To specify that archiving should apply for a specific camera, select the check box next to the name of the required camera. Specifying that archiving should apply for a specific camera Remember that only when you click *OK* is archiving actually enabled for the selected cameras. **Archiving Locations for Individual Cameras (Static archiving)** If the *Automatic path selection* check box is not selected, you must specify an archiving location for each camera. This is further described under *Static Archiving* (see page 133). **Archiving Locations for All Cameras (Dynamic Archiving)** By selecting the Automatic path selection check box, you can specify archiving locations for all selected cameras in one go to a number of drives on your network. Archiving will take place dynamically to all selected drives. This is further described under *Dynamic Archiving* (see page 134).
Set all	Selects the check boxes for all cameras listed in the *Select cameras for which the archiving function should apply* section. Clicking the *Set all* button is thus a quick way to specify that archiving should apply for all cameras listed. Remember that only when you click *OK* is archiving actually enabled for the selected cameras.
Clear all	Clears the check boxes for all cameras listed in the *Select cameras for which the archiving function should apply* section. Clicking the *Clear all* button is thus a quick way to specify that archiving should not apply for any of the cameras listed. Remember that only when you click *OK,* archiving is actually disabled for the selected cameras.
Set all paths	**Note:** This button is only available if the *Automatic path selection* check box is cleared. Copies the selected path listing to all cameras listed in the *Select cameras for which the archiving function should apply* section. If you use the same archiving directory for all cameras, this can save you having to manually specify identical paths for each camera. Example: You have specified the path C:\MyFiles\MySurveillanceSystem for a camera. To quickly use this path for all cameras, select the path listing and click the *Set all paths* button.
Add target	**Note:** This button is only available if the *Automatic path selection* check box is selected.

Field, Button	Description
	By clicking this button, you can add a new archiving target. When you click the button, a path named *New drive* will appear in the list. To specify a path simply click *New drive* to overwrite it. The path you type **must** exist in the *My Network Places* folder. Note, that the path you type will not get a drive letter. That is because it is not a mapped drive. If it had been a mapped drive, it would already have been in the list.  **Note:** You cannot delete a target you have added. Instead, if you clear a check box for a target you have added manually and click *OK*, the target will not be on the list the next time you access the *Archive setup* window. However, the *Archives* folder at the target destination will remain available for viewing recordings.

Tip: Milestone's *Storage Calculator*, found in the support section of the Milestone website, www.milestonesys.com, can help you easily determine the storage capacity required for your surveillance system.

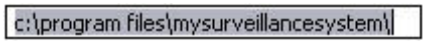
Static Archiving

Specifying archiving locations for individual cameras is only possible when the *Automatic path selection* check box is not selected.



If the *Automatic path selection* check box is not selected, a default archiving location (typically c:\program files\milestone\milestone surveillance\) is specified for each camera. The default archiving directory, called *Archives*, will be located at this location.

To specify another location for the archiving directory for a camera, either click the *browse* icon next to the path listing for the required camera and browse to the required location, or click the default path listing to overwrite it.



Overwriting an existing path

Tip: To maximize load sharing and optimize performance, distribute archives across your available storage space, if possible.

Note: If specifying another archiving location than the default location (typically c:\program files\milestone\milestone surveillance\), the location you specify must exist. You are not able to create new directories as part of the process. If archiving to a network drive, the regular camera database **must** still be stored on a local drive, i.e. a drive attached directly to the computer running the XProtect Enterprise system.

Archives for the selected camera will be stored in separate subdirectories under the *Archives* directory at the location you specify. The subdirectories will be named according to the following structure:

```
...\Archives\CameraMACAddress_VideoEncoderChannel\DateAndTime
```

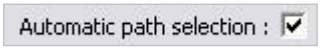
Example: With the default archiving folder located under C:\MyFiles\MySurveillanceSystem, recordings from an archiving taking place at 23.15 on 1st June 2005 for a camera attached to channel 2 on a video server device with the MAC address 00408c51e181 would be stored at the following destination:

```
C:\MyFiles\MySurveillanceSystem\Archives\00408c51e181_2\2005-06-01-23-15
```

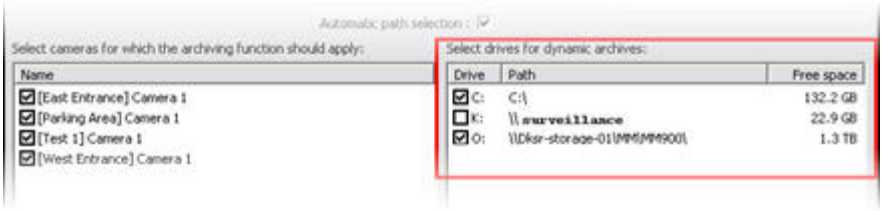
If the device to which the camera is attached is not a video encoder device with several channels, the video encoder channel indication in the subdirectory named after the device's MAC address will always be *_1*. Example: 00408c51e181_1.

Dynamic Archiving

Dynamic archiving is ideal if you wish to archive to several drives during the same archiving process but do not want to worry about how much space is used on each drive. Dynamic archiving is only possible when you select the *Automatic path selection* check box.



When you select *Automatic path selection*, you will be able to specify archiving locations for all selected cameras in one go. In the *Select drives for dynamic archives* section, simply select the box next to each drive required as archives.



Note that it is only possible to select drives; you cannot edit the paths. An *Archives* directory will automatically be created in each drive, and the archiving will take place the same way as described previously under *Specifying that Archiving Should Apply for Specific Cameras*.

If you need to use a path for archiving that is not in the list, click the *Add target* button.

What Happens During Dynamic Archiving?

If the drive on which the camera stores its regular database is among the drives you have selected for dynamic archiving, archiving for the camera in question will always take place to that drive first. If the drive on which the camera stores its regular database is or becomes full—or if it is simply not among the drives selected for dynamic archiving—archiving will take place to the selected drive with the most free disk space. Which drive that is may change during the archiving process, and archiving may therefore happen to several drives during the same process. However, that has no impact on how you find and view archived recordings.

Note: If you use a drive for both recording and archiving, archiving to that drive will only take place from cameras recording to that drive. In that case, you should select one or more other drives for archiving, so that archiving from other databases will also take place. Alternatively, you should avoid using the same drive for both recording and archiving.

IMPORTANT: If you have more that one surveillance server, each surveillance server *must* archive to its own mapped location in order for archiving to work. If you try to archive to the same mapped location from all the servers, archiving will not work.

Archiving Audio

If audio is enabled on a device, audio from the device will also be archived. If the device is a video encoder with several channels, audio will be archived with the camera on channel 1.

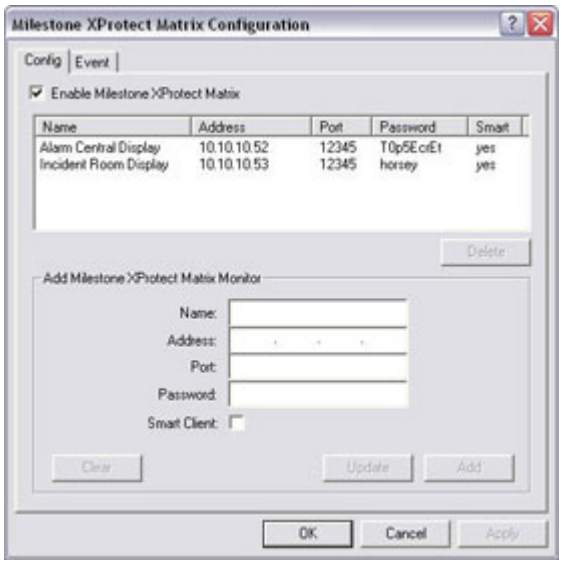
Matrix Administration

Matrix Configuration Window

Matrix allows distributed viewing of live video from any camera on any monitor on a network operating with XProtect Enterprise.

A computer on which Matrix-triggered video can be displayed is known as a Matrix recipient. Being able to view Matrix-triggered video requires that either a *Smart Client* (see page 175) or the dedicated *Matrix Monitor* software is installed on the user's computer.

You access the *Matrix Configuration* window by clicking the *Matrix...* button in the *Administrator* window (see page 30).



The *Matrix Configuration* window has two tabs:

- The ***Config*** tab lets you define individual computers on which it should be possible to view Matrix-triggered content (such computers are known as Matrix recipients)
- The ***Event*** tab lets you define which events should trigger which actions in individual Matrix recipients

Enabling Matrix and Defining Matrix Recipients

The *Config* tab is used for enabling Matrix functionality and for defining which computers to display Matrix-triggered live video on.

The *Config* tab contains the following fields, check boxes and buttons:

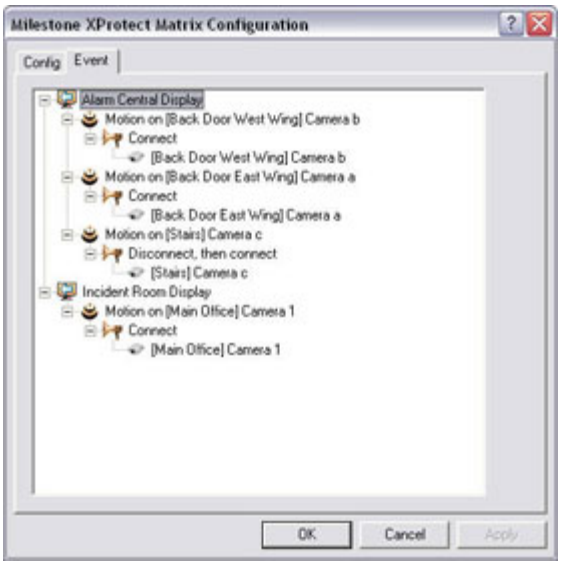
Field, Check Box, Button	Description
Enable Milestone XProtect Matrix	Select check box to enable Matrix functionality.
[List of Defined Matrix recipients]	Lists any already defined Matrix recipients, i.e. computers on which Matrix-triggered video can be displayed. To change the properties of an already defined Matrix recipient, select the required Matrix recipient, make the changes in the fields below the list, then click the *Update* button. To remove a Matrix recipient from the list, select the unwanted Matrix

Field, Check Box, Button	Description
	recipient, then click the *Delete* button. You will be prompted to confirm the removal.
Delete	Available only when you have selected a Matrix recipient in the list. Clicking the *Delete* button will remove the selected Matrix recipient. You will be prompted to confirm the removal.
Name	Used when adding a new Matrix recipient or editing the properties of an existing one. Type a name for the Matrix recipient. The name will appear in various day-to-day usage situations; it is therefore a good idea to use a descriptive and unambiguous name. **Note:** Matrix recipient names must not contain the following characters: < > & ‘ " \ / : * ? | [ ]
Address	Used when adding a new Matrix recipient or editing the properties of an existing one. Specify the IP address of the Matrix recipient. To jump to the next IP address segment in the field, press SPACE on your keyboard.
Port	Used when adding a new Matrix recipient or editing the properties of an existing one. Specify the port number to be used when sending commands to the Matrix recipient. The Matrix recipient will listen for commands on this port. By default, port 12345 is used. You are of course able to specify another port number.
Password	Used when adding a new Matrix recipient or editing the properties of an existing one. Specify the password to be used when communicating with the Matrix recipient.
Smart Client	Matrix-triggered live video may also be displayed in users' Smart Clients (see page 175). If a Smart Client is used, distribution of the Matrix-triggered live video takes place slightly differently. Select check box if the Matrix recipient in question is a Smart Client.
Clear	Removes any content in the *Name*, *Address*, *Port*, *Password* and *Smart Client* fields.
Update	Available only if you have edited the properties of an existing Matrix recipient. Updates the properties of the selected Matrix recipient with the changes made during editing.
Add	Available only if you have added properties of a new Matrix recipient in the *Name*, *Address*, *Port*, *Password*, and possibly Smart Client fields. Adds the new Matrix recipient to the list.

Automatic Matrix Display on Events

There are two ways in which Matrix-triggered video can appear in a Matrix recipient:

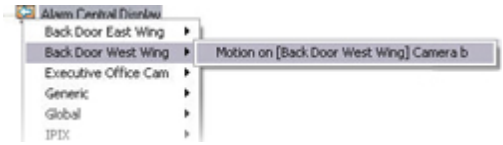
- Another user wants to share important video, and sends it to the required Matrix recipient from a *Smart Client*, or from a custom-made web page
- Video is sent to the required Matrix recipient automatically when a predefined event occurs



The *Event* tab is used for configuring the automatic sending of live video based on predefined events; it lets you define exactly which events and cameras to use. You define this on a per-Matrix recipient basis.

To define what should happen on which Matrix recipient when an event occurs, do the following:

1. Select the required Matrix recipient.
2. Right-click the Matrix recipient to select the required event:



In this example, the selected event is detected motion on a particular camera. Note that, if available, you are also able to select other types of event, including input events, generic events, VMD events, event buttons (including global event buttons) and timer events.

When you select an event, it will initially be highlighted by a red exclamation mark:

The exclamation mark indicates that there is additional configuration to be done.

3. Now right-click the event to select which action should take place when the event occurs:

Alarm Central Display
Motion on [Back Door West Wing] Camera b
Delete Motion on [Back Door West Wing] Camera b
Connect
Disconnect, then connect
Disconnect

You have three actions to choose from:

- ***Connect*:** Connect to the camera (you will specify the actual camera in the next step)
- ***Disconnect, then connect*:** Disconnect any existing connection to the camera (you will specify the actual camera in the next step), then connect again.

  This option is useful because Matrix recipients are often able to show live video from more than one event, in which case the live video will appear in the Matrix

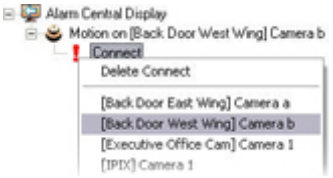
recipient on a first-in-first-out basis. Each time a new event occurs, video from the latest event is displayed prominently in a specific position on the Matrix recipient, while at the same time video from the older events is shifted to less prominent positions and eventually "pushed out" of the Matrix recipient in order to make space for the latest event's video.

With the *Connect* option, you may thus experience that if video triggered by one event on a camera is already shown on the Matrix recipient, videos triggered by another event on the same camera would not be displayed prominently as coming from the latest event – simply because the Matrix recipient is already showing video from the camera in a less prominent position. By selecting *Disconnect, then connect* you can avoid this issue, and ensure that video from the latest event is always displayed prominently.

- ***Disconnect*:** Disconnect the camera (you will specify the actual camera in the next step). Use if a particular event should cause video from a particular camera to stop being displayed in the Matrix recipient, even if it is not yet old enough to be "pushed out" of the Matrix recipient.

When you have selected an action, another red exclamation mark will indicate that there is still some configuration to be done:

4. Right-click the action to select which camera to apply the action on:


Alarm Central Display
Motion on [Back Door West Wing] Camera b
Connect
Delete Connect
[Back Door East Wing] Camera a
[Back Door West Wing] Camera b
[Executive Office Cam] Camera 1
[IPIX] Camera 1

In this example, we have specified that when motion is detected on Camera b, the selected Matrix recipient should connect to Camera b:

5. Repeat as required. Bear in mind that you define events and actions for a single Matrix recipient at a time.

Image Server Administration

Image Server Administrator Window

The *Image Server* provides access to the surveillance system for remote users logging in with a Remote Client (see page 178) or a Smart Client (see page 175). If the PDA Server (see page 179) front end is installed, the *Image Server* also handles access for *PDA Client* users.

The *Image Server* itself does not require separate hardware; it runs as a service on the surveillance system server (i.e. the computer running the XProtect Enterprise software). Surveillance system administrators use the *Image Server Administrator* window to manage the *Image Server*'s settings.

You access the *Image Server Administrator* window from Windows' *Start* menu: Select *Start* > *All Programs* > *Milestone XProtect Enterprise* > *Image Server Administrator*. Alternatively, simply double-click the *Image Server Administrator* desktop shortcut.

Each section of the *Image Server Administrator* window is described in the following:

Server Configuration Section

The *Server Configuration* section is used for specifying server name and port, for enabling optional external access to the server, for optional definition of IP address ranges which should be recognized as being local, and for specifying a maximum number of remote users allowed to connect simultaneously.

Field, Button	Description
Name	Lets you specify a name for the server. By default, the name is simply *Server*. You can of course change the default name to a name of your choice. Remote Client and Smart Client users with rights to configure their clients will see the name of the server when they create views on their client's *Setup* tab.
Port	Lets you specify a port number to use for the server. The default port number is 80. You are able to change the default port number.
Enable Outside Access	Select the check box if the server should be accessible from the internet via a router or firewall. If selecting this option, also specify the outside (public) IP address and port number in the *Outside IP Address* and *Outside Port* fields. **Note:** When using outside access, the router or firewall used must be configured so requests sent to the outside (public) IP address and port are forwarded to the inside (local) IP address and port of the server running the *Image Server* service.

Outside Address	Lets you specify a public IP address or host name for use when the server should be available from the internet.
Outside Port	Lets you specify a port number for use when the server should be available from the internet. The default port number is 80. You are able to change the default port number.
Local IP Ranges...	Opens the *Define local IP ranges* window (see page 144), in which you are able to define IP address ranges which the *Image Server* should recognize as coming from a local network. Background: When a Remote Client *or* Smart Client connects to a surveillance system, an amount of initial data communication, including the exchange of contact IP addresses goes on in the background, completely automatically and transparent to users. However, when a Remote Client or Smart Client on a local network connects to a surveillance system which is also on the local network, the Image Server may, if different subnets are involved, not recognize the Remote Client's or Smart Client's IP address as being local. When this is the case, the Image Server may not return a suitable IP address to the Remote Client or Smart Client for further communication between the two. Therefore, you are able to define a list of IP ranges which the Image Server should recognize as coming from a local network, in which case it will respond with a suitable IP address and seamless communication will be possible.
Max. number of clients	You are able to limit the number of access clients allowed to connect at the same time. Depending on your XProtect Enterprise configuration and the performance of the hardware and network used, limiting the number of simultaneously connected clients may help reduce server load. If more than the allowed number of simultaneously connected access clients attempt to log in, only the allowed number of access clients will be allowed access. Any access clients in excess of the allowed number will receive an error message when attempting to log in. By default, a maximum of ten simultaneously connected access clients are allowed. To specify a different maximum number of access clients allowed to connect at the same time, overwrite the value in the *Max. number of clients* field with the required value. **Tip:** To allow an unlimited number of simultaneously connected access clients, type *0* (zero) in the *Max. number of clients* field. **Note:** A four-minute session timeout period applies for access client sessions on the Image Server. In many cases, access client users may not notice this at all. However, the session timeout period will be very evident in some cases, for example if you set the *Max. number of clients* value to *1*: When this is the case, and the single allowed access client user logs out, four minutes must pass before it will be possible to log in again.

User Administration Section

Accounts and rights for access client users are configured in the *Image Server Administrator* window's *User Administration* section. Access client users must be defined in this section in order to be able to log in to the surveillance system.

Defining Users

To define access client users, click the *User Setup* button. This will open the *User administration* window (see page 144), in which you define users.

Defining User Access Rights

Once you have defined users, you are able to define whether all users should have access to all features in their access clients, including all available cameras, or whether access should be restricted on an individual user basis.

Full Access for All Users

To give all users access to all features and all available cameras, select *Full access for all users*.

Restricted Access

To use restricted access, select *Restrict user access*. Then click the *User Access...* button to open the *Define User Rights* window (see page 148), in which you define access rights for each user.

Master/Slave Setup Section

You are able to create a master/slave setup of XProtect Enterprise servers. A master/slave setup will allow remote users to transparently connect to more than one server simultaneously: When remote users connect to the master server, they will instantly get access to the slave servers as well.

How many *master* servers can I use in a master/slave setup? An unlimited number of servers per SLC (Software License Code, specified during installation) can be designated as master servers. If required—for example if your organization is very large and spread over many geographical locations, or in case you want to create a redundancy solution—this allows you to use several master servers in a master/slave setup.

How many *slave* servers can I use in a master/slave setup? An unlimited number of servers can be defined as slave servers under a designated master server using the same Software License Code.

Note: When using a master/slave setup, remote users and their rights must be defined in the *Image Server Administrator* window on the master server as well as on each of the slave servers. Only cameras to which a remote user has been given access will be visible to the user, regardless of whether the cameras are connected to the master server or to one of the slave servers.

Note: If they are to be accessed from the internet, *Enable Outside Access* must be selected on all involved servers, and ports must be mapped accordingly in the routers and/or firewalls used.

Note: If upgrading the XProtect Enterprise servers involved in a master/slave setup to XProtect Enterprise 6.0 or later from a previous XProtect Enterprise version, a certain procedure is recommended. Read *Upgrading Servers in an Existing Master/Slave Setup* on page 142 for more information.

Configuration on the Master Server

If the server you are configuring should be a master server, do the following:

1. Select the *Designate as Master Server* check box.

2. Next, define which other XProtect Enterprise servers should act as slave servers. To define other servers as slave servers, click the *Slaves...* button:

   This will open the *Slave Administration* window (see page 151), in which you are able to define all required slave servers.

Configuration on a Slave Server

Apart from the notes listed above, no special master/slave configuration is required on a slave server; simply do not specify anything in the *Master/Slave Setup* section:

If Not Using a Master/Slave Setup

If you do not wish to use a master/slave setup—for example because there is only a single XProtect Enterprise server on your system—simply do not specify anything in the *Master/Slave Setup* section.

Upgrading Servers in an Existing Master/Slave Setup

The servers involved in a master/slave setup should preferably all use the latest XProtect Enterprise version. If you only upgrade to XProtect Enterprise 6.0 or later on the master server while letting the slave servers run a previous version (e.g. XProtect Enterprise 5.6), access client users will lose access to key functionality in their client applications.

It is therefore highly recommended that you upgrade *all* the servers involved in an existing master/slave setup to XProtect Enterprise 6.0 or later.

When you do this, a certain procedure is recommended. The procedure ensures that remote users will not experience any loss of functionality, not even during a transition period in which some servers may run XProtect Enterprise 6.0 or later while other servers still run a previous XProtect Enterprise version:

1. Install XProtect Enterprise 6.0 or later on the **master** server.

2. In the *Image Server Administrator* window on the **master** server, select the *Pre-6.0 Version Slaves* check box:

3. Click *OK* to close the **master** server's *Image Server Administrator* window, thus restarting the *Image Server* service.

4. Upgrade the **slave** servers to XProtect Enterprise 6.0 or later.

5. When *all* of the **slave** servers have been upgraded, clear the *Pre-6.0 Version Slaves* check box on the **master** server, and click *OK* to close the **master** server's *Image Server Administrator* window, thus restarting the *Image Server* service.

Keep Transition Period as Short as Possible

It is recommended that you keep the transition period as short as possible, as client connections' security will be considerably stronger once all servers involved in the master/slave setup have been upgraded to XProtect Enterprise 6.0 or later, and the master server's *Pre-6.0 Version Slaves* check box has been cleared.

Also, while the *Pre-6.0 Version Slaves* check box is selected, the *Image Server Administrator* window's *Max. Number of Clients* feature will only apply for Remote Clients, not for Smart Clients.

Log Files Section

In the *Log Files* section, specify the number of days to keep log files in the Image Server's regular event log. By default, such log files are kept for ten days before they are deleted.

Tip: Read more about logging on page 157.

Audit Log Section

Audit logging is the logging of access client user actions. If this type of logging is required, select the *Enable Audit Logging* check box. When audit logging is enabled, you are able to specify the following values:

- ***Days to log*:** Number of days in which audit log files should be kept before they are overwritten. Default is 30 days. If you specify 0 (zero), audit log files will be kept indefinitely (disk storage space permitting).
- ***Minimum Logging Interval*:** Minimum number of seconds between logged events. Specifying a high number of seconds between logged events may help reduce the size of the audit log. Default is 60 seconds.
- ***In Sequence Timespan***: Maximum number of seconds to pass for viewed images to be considered to be within the same sequence. Specifying a high number of seconds may thus help limit the number of viewed sequences logged, and reduce the size of the audit log. Default is ten seconds.

Language Support and XML Encoding Section

In the *Language Support and XML Encoding* section, select the language/character set used by the XProtect Enterprise server and access clients.

Example: If the XProtect Enterprise server runs a Japanese version of Windows, select *Japanese*. Provided access clients also use a Japanese version of Windows, this will ensure that the right language and character encoding is used in clients' communication with the server.

If using a master/slave setup, remember to specify the same language/character set on all involved servers.

Good to Know: Client Access to Stopped Cameras

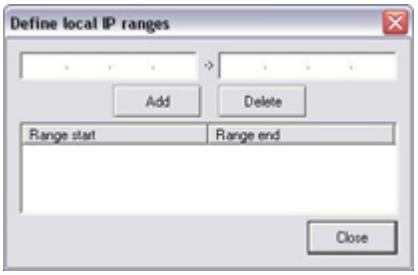
Access client users are able to view live video from cameras even though the cameras in question are not online (online means that the camera delivers a video stream to the surveillance system server, as defined in the Camera/Alert Scheduler Window, see page 71). This, however, requires that a particular setting in the Administrator application is enabled. To enable the required setting, open the Administrator application, and do the following:

1. In the *Administrator* window (see page 30), click the *General Settings...* button. This will open the *General Settings* window (see page 76).

2. In the *General Settings* window's *Advanced* section, select *Start cameras on remote live requests*.

3. Click *OK*.

Define Local IP Ranges Window



The *Image Server Administrator*'s *Define local IP ranges* window lets you define IP address ranges which the Image Server should recognize as coming from a local network.

You access the *Define local IP ranges* window by clicking the *Local IP Ranges...* button in the *Image Server Administrator* window (see page 139).

To define a local IP address range in the *Define local IP ranges* window, do the following:

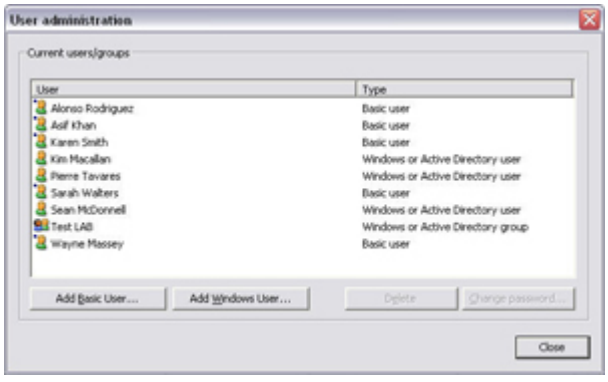
1. Specify the beginning of the IP address range in the *Define local IP ranges* window's first field, and the end of the IP address range in the second field.

2. Click the *Add* button. The IP address range will be added to the list in the lower part of the *Define local IP ranges* window. You may define as many local IP address ranges as required. If required, an IP address range may include only one IP address (example: 192.168.10.1-192.168.10.1).

3. When ready, click the *Define local IP ranges* window's *Close* button to return to the *Image Server Administrator* window.

Tip: There is no feature for editing an already defined IP address range in the *Define local IP ranges* window. However, you can simply select the range in question in the *Define local IP ranges* window's list, delete it by clicking the *Delete* button, and then simply add a new range reflecting your requirements.

User Administration Window



The *Image Server Administrator*'s *User administration* window lets you define access client users. You access the *User administration* window by clicking the *User Setup...* button in the *Image Server Administrator* window (see page 139). You are able to add new users in two

ways, which may be combined.

- ***Basic user*:** Lets you create a dedicated surveillance system user account with basic user name and password authentication for each individual user. If the PDA Server (see page 179) is installed, this method works for PDA Client users.

- ***Windows user*:** Lets you import individual users or groups defined locally on the server, or users/groups from Active Directory, and authenticate them based on their Windows login. This method does not work for PDA Client (see page 179) users. Using Active Directory requires that a server with Active Directory installed and acting as domain controller is available on your network

What Is Active Directory?

Active Directory is a distributed directory service included with several Windows Server operating systems; it identifies resources on a network in order for users or applications to access them. Users and, if required, groups of users are specified centrally in Active Directory.

In short, the benefits of importing user data from Active Directory are that: Administrators do not have to create separate user accounts for accessing the surveillance system because user authentication will be handled centrally by Active Directory. Administrators can import groups of users in one go if required. Users can basically just use their Windows login when accessing the surveillance system; no need to memorize separate user names and passwords.

Prerequisites

The Image Server managing the remote access verifies Smart Client (see page 175) users' identities using NTLM challenge handshake with a Microsoft Domain Controller. In order to be able to import users and groups through Active Directory, a server with Active Directory installed and acting as domain controller must be available on your network. Consult your network administrator if in doubt.

User and Group Concepts

Active Directory uses the concepts of users and groups. Users are Active Directory objects representing individuals with a user account. Example:

Groups are Active Directory objects that can contain several users. In this example the Management group contains three users:

Groups can contain any number of users. By importing a group into XProtect Enterprise, you are able to import all of its members in one go. The number of groups may vary from organization to organization, depending on the structure and requirements of each organization. Note that a user can be a member of more than one group. For instance, Adolfo Rodriguez from our fictitious example above could easily be a member of the organization's Management group as well as of its Sales group and its Staff Social Club group.

Each of the two methods is described in the following:

How to Add a New Basic User

To define a new dedicated surveillance system user account with basic user name and password authentication, click the *User administration* window's *Add Basic User...* button, specify required user name and password, and click *OK*.

This will add the user to the *User administration* window's list of users. In the list's *Type* column, the user will appear as a *Basic User*. A *Basic user* is furthermore indicated by a blue dot next to the user icon. Example:

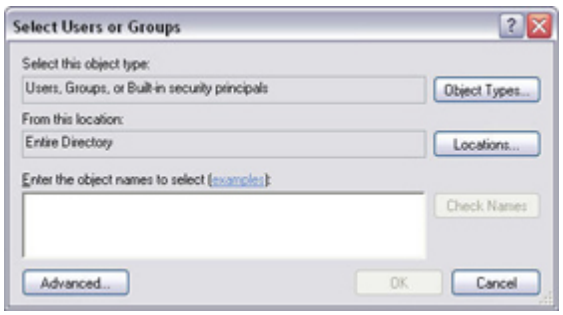
How to Add a New Windows User or Group

Note: This method only works for users who will access the surveillance system through the *Smart Client* (see page 175) or *Remote Client* (see page 178). If your users will access the surveillance system with a *PDA Client* (see page 179), add the users as *Basic users* instead.

You add a new Windows user or group by importing information about the user/group from a local database on the surveillance system server or from Active Directory:

1. In the *User administration* window, click the *Add Windows User...* button. This will open the *Select Users or Groups* window.

   By default, you will be able to make selections from your entire directory. If you want to narrow this, click the *Select Users and Groups* window's *Locations...* button, and select the location you require.

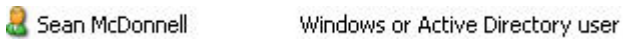


2. In the *Enter the object names to select* box, type the required user or group names, then use the *Check Names* feature to verify that the user and/or group names you have entered are recognized by Active Directory.

   Note: If typing several user and/or group names, separate each name with a semicolon. Example: *Alonso; Sarah Walters; Management; Brian; Security; Hannah Carter; Stanislaw; Dwayne Smith*

   Tip: Typing part of a user or group name is often enough. Example: Typing *Alon*, then clicking the *Check Names* button, may be enough to quickly select the user *Alonso Rodriguez*.

3. When ready, click *OK*. The required users and/or groups will be imported, and listed in the *User administration* window. A *user* imported this way will appear as a *Windows or Active Directory User* in the list's *Type* column. The user will furthermore be indicated by a user icon *without* the blue dot used for *Basic users*. Example:



A *group* imported this way will appear as a *Windows or Active Directory Group* in the list's *Type* column. The group will furthermore be indicated by a group icon. Example:

How to Edit an Existing User Name or Password

Editing an existing user's user name or password is only possible if the user in question is of the type *Basic user*; the details of *Windows users* imported from Active Directory are edited through Active Directory.

1. Select the required user in the *Current users* list, and click the *Change password...* button.

2. Edit the user name and/or password as required, then click *OK*. Remember to inform the user about the change.

How to Remove an Existing User

To remove a user from the *User administration* window's list of users, select the user in the list and click the *Delete* button. When removed from the list, the user will no longer be able to log in.

Note: Using this method to delete a *Windows user* imported from Active Directory will only remove the user's right to log in with a Milestone XProtect access client; it will not remove the user's data from Active Directory.

What Information to Provide to Users

The information you need to provide in order to enable users to effortlessly log in to the surveillance system depends on whether the users are using Remote Clients or Smart Clients. If you have PDA Client users, see more about the PDA Server and Client on page 179.

Remote Client Users

When users log in with *Remote Clients*, they must select between using basic or Windows-based authentication. Provide them with the following information:

- ***Address***: IP address or hostname of the *Image Server*.

- ***Port*:** Port to use when accessing the *Image Server*, e.g. 80.

- ***Authentication***: In the *Remote Client*'s login dialog, users will be asked to select between basic authentication or Windows-based authentication. Windows-based authentication may in turn be based on the currently logged-in Windows user.

    - If using basic user name and password authentication, tell users that the required authentication is called *Basic*.

    - If using Windows-based authentication based on the currently logged-in Windows user, tell users that the required authentication is called *Windows (current user)*.

    - If using Windows-based authentication which should not necessarily be based on the currently logged-in Windows user, tell users that the required authentication is called *Windows*.

- ***User name:*** *Only required if using Basic authentication or Windows authentication.* Remember that user names are case sensitive, so make it clear to the users if any parts of

their user names should specifically be upper or lower case.

- ***Password*:** *Only required if using Basic authentication or Windows authentication*. If using *basic authentication*, users should enter their passwords exactly as you have specified them on the *Image Server*.

Smart Client Users

When users log in with *Smart Clients*, they must select between using basic or Windows-based authentication. Provide them with the following information:

- ***Server Address*:** IP address or hostname of the *Image Server*, plus any port number required. In the *Smart Client*'s login dialog, users will enter this information in a single field called *Server Address*, so if the IP address is 123.123.123.123 and the port number is 80, tell users that the *Server Address* is 123.123.123.123:80.

- ***Authentication***: In the *Smart Client*'s login dialog, users will be asked to select between basic authentication or Windows-based authentication. Windows-based authentication may in turn be based on the currently logged-in Windows user.

    - If using basic user name and password authentication, tell users that the required authentication is *Basic authentication*.

    - If using Windows-based authentication based on the currently logged-in Windows user, tell users that the required authentication is *Windows authentication (current user)*.

    - If using Windows-based authentication which should not necessarily be based on the currently logged-in Windows user, tell users that the required authentication is *Windows authentication*.

- ***User name*:** *Only required if using Basic authentication or Windows authentication*. Remember that user names are case sensitive, so make it clear to the users if any parts of their user names should specifically be upper or lower case.

- ***Password*:** *Only required if using Basic authentication or Windows authentication*. If using basic authentication, users should enter their passwords exactly as you have specified them on the *Image Server*.

    - Users with *Basic authentication* or *Windows authentication* will have the option of selecting *Remember password*, which will help them speed up subsequent login procedures. Inform users whether they are allowed to use this feature.

- ***Auto-login*:** Users will have the option of selecting *Auto-login*, in which case the *Smart Client* (see page 175) will automatically start up and log in with the selected authentication method each time Windows is started (for *Basic authentication* and *Windows authentication* this will require that *Remember password* is selected). Inform users whether they are allowed to use this feature.

Define User Rights Window

The *Image Server*'s *Define User Rights* window lets you define access rights for access client users. You access the *Define User Rights* window by clicking the *User Access...* button in the *Image Server Administrator* window (see page 139). The button is only available if you have selected the *Image Server Administrator* window's *Restrict user access* option button.

Prerequisites: Before you define user rights, you should define users. You do this by clicking the *Image Server Administrator* window's *User Setup...* button.

To define access rights for a particular user, do the following in the *Define User Rights* window:

1. In the *User* list, select the required user (or—if groups of users have been imported through Active Directory—group (see page 144)).

2. In the *Global User Rights* section, select the user's/group's global (i.e. non-camera-specific) rights:

   - ***View Live*:** Ability to view the *Live* tab in the Remote Client/Smart Client. If a user/group does not have this right, the *Live* tab will not be selectable in the Remote Client/Smart Client.

   - ***Browse*:** Ability to view the *Browse* tab in the Remote Client/Smart Client. If a user/group does not have this right, the *Browse* tab will not be selectable in the Remote Client/Smart Client.

   - ***Setup*:** Ability to view the *Setup* tab in the Remote Client/Smart Client. If a user/group does not have this right, the *Setup* tab will not be selectable in the Remote Client/Smart Client.

   - ***Edit Shared Views*:** Ability to create and edit views in shared groups in the Remote Client/Smart Client. Views placed in shared groups can be accessed by every Remote Client/Smart Client user (for more information about views, see the separate Remote Client or Smart Client documentation). If a user/group does not have this right, shared groups in the Remote Client/Smart Client will be protected, indicated by a padlock icon.

     Note: Views created in a Remote Client can only be shared with other Remote Client users. Views created in a Smart Client can only be shared with other Smart Client users. It is not possible to share views across the two types of client.

   - ***Edit Private Views*:** Ability to create and edit views in private groups in the Remote Client/Smart Client. Views placed in private groups can only be accessed by the Remote Client/Smart Client user who created them (for more information about views, see the separate Remote Client or Smart Client documentation). If a user/group does not have this right, private groups in the Remote Client/Smart Client will be protected, indicated by a padlock icon. Denying remote users the right to create their own views may make sense in some cases; for example in order to limit bandwidth use.

   Tip: By clearing the *View Live*, *Browse* and *Setup* check boxes you can effectively disable the user's/group's ability to use the Remote Client/Smart Client, for example while the user is on vacation. This would typically be a temporary alternative to deleting the user/group.

3. In the *User Rights for Camera* section's *Defined Cameras* list, select each camera to which the user/group should have access in the access client.

   Tip: By pressing the CTRL or SHIFT buttons on your keyboard while selecting cameras, you are able to select several or all of the listed cameras in one go.

4. Click the >> button to move the selected cameras to the *Viewable by selected user* list.

5. For **each** camera now listed in the *Viewable by selected user* list, specify the features to which the user/group should have access, by selecting the features in the *User Rights for the Selected Camera* section. Note that the features are listed in two columns: the left column lists features related to live viewing, the right column lists features related to browsing existing recordings:

   In the *Live* column, the following features, all selected by default, are available:

   - ***Live*:** Ability to view live video from the selected camera.
   - ***PTZ*:** Ability to use navigation features for PTZ (Pan/Tilt/Zoom) cameras. A user/group will only be able to use this right if having access to one or more PTZ cameras.
   - ***PTZ Preset Positions*:** Ability to use navigation features for moving a PTZ camera to particular preset positions. A user/group will only be able to use this right if having access to one or more PTZ cameras with defined preset positions.
   - ***Outputs*:** Ability to trigger outputs (e.g. switching on lights, sounding sirens, or similar), if such outputs are available.
   - ***Events*:** Ability to use the Smart Client' *Event* feature for manually triggering events. The *Event* feature is available in the Smart Client (see page 175) only.
   - ***Listen to microphone:*** Ability to listen to live audio from the selected camera's microphone(s) (available only if the selected camera has microphone(s) attached). The *Listen to microphone* feature is available in the Smart Client only.
   - ***Talk to speaker:*** Ability to talk to the selected camera's speaker(s) (available only if the selected camera has speaker(s) attached). The *Talk to speaker* feature is available in the Smart Client only.

   In the *Browse* column, the following features, all selected by default, are available:

   - ***Browse*:** Ability to browse recorded video from the selected camera.
   - ***AVI / JPG Export*:** Ability to generate and export evidence as movie clips in the AVI format and as still images in the JPG format.
   - ***Database Export*:** Ability to generate and export evidence in database format. The *Database Export* feature is available in the Smart Client only.
   - ***Sequences*:** Ability to use the *Sequences* feature for browsing video from a selected camera.
   - ***Smart Search*:** Ability to use the Smart Client's *Smart Search* feature, with which users are able to search for motion in one or more selected areas of images from the selected camera. The *Database Export* feature is available in the *Smart Client* only.
   - ***Audio*:** Ability to listen to recorded audio from the selected camera's microphone(s) (available only if the selected camera has microphone(s) attached) The *Audio* feature is available in the Smart Client only.

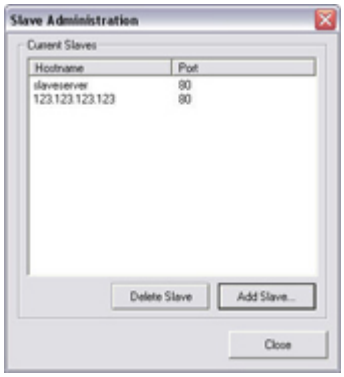
   Tip: Note that some of the features are mutually dependent: For example, in order have access to PTZ or output features, a user must also have access to viewing live video;

and in order to use AVI and JPG export, a user must have access to browsing recorded video.

6. Repeat as required for other users/groups.

What if a user is a member of a group which has different rights than the user itself? When this is the case—for example when the user Paul himself has been given rights to do A and B, whereas the Security Staff group of which Paul is a member has been given rights to do A, B, and C—the sum of the rights will apply for the user. Paul in our example would then—due to his group membership—have rights to do A, B, and C.

Slave Administration Window



The *Image Server Administrator*'s *Slave Administration* window lets you define all servers required to run as slave servers under the XProtect Enterprise server you are configuring. Remember that only one server can be the master server. Any number of servers can be defined as slave servers under the master server. You access the *Slave Administration* window by clicking the *Slaves...* button in the *Image Server Administrator* window (see page 139).

Adding a Slave Server

To add a slave server, click the *Slave Administration* window's *Add Slave...* button, specify the host name of the slave server, specify the required port number, and click *OK*. This will add the slave server to the *Slave Administration* window's list of slave servers.

Tip: Instead of specifying a host name when adding a slave server, you may specify the IP address of the slave server. Simply type the IP address in the *Hostname* field when adding the slave server. Remember that if on a local network, the *local* IP address of the slave server must be used.

Before you start using your master/slave setup, remember to verify that:

- Required users have been defined on the master server as well as on each of the slave servers.
- *Outside Access* has been enabled on all involved servers, and ports mapped accordingly in the routers or firewalls used, if the slave servers are to be accessed from the internet.

Removing a Slave Server

To remove a slave server from the *Slave Administration* window's list of slave servers, select the slave server in the list and click the *Delete Slave* button.

End-User Documentation

For end-user documentation about how to configure and use the *Remote Client* and *Smart Client*, see the separate manuals *Milestone XProtect Remote Client User's Manual* and *Milestone XProtect Smart Client User's Manual*. The manuals are available on the XProtect Enterprise software DVD as well as on www.milestonesys.com.

Download Manager

The Download Manager lets you manage which XProtect Enterprise-related features your organization's users will be able to access from a targeted welcome page on the surveillance system server. You access the Download Manager from Windows' *Start* menu: Select *All Programs > Milestone XProtect Download Manager > Download Manager*.

Examples of user-accessible features:

- The Smart Client (see page 175). With a regular Internet Explorer browser, users connect to the surveillance server where they are presented with a welcome page. From the welcome page, users can download the Smart Client software and install it on their computers.
- Language packs, which let users add additional language versions to their existing Smart Clients. Users download such language packs from the welcome page.
- The Remote Client (see page 178). Users connect to welcome page and log in to the Remote Client, which simply runs in a browser without any need for software installation.
- Various plugins. Downloading such plugins can be relevant for users if your organization uses add-on products with the XProtect Enterprise solution.

The Welcome Page

The welcome page is a simple web page with links to downloading or running various features. It is available in a number of languages; users select their required language from a menu in the top right corner of the welcome page.

To view the welcome page, simply open an Internet Explorer browser (version 6.0 or later) and connect to the following address:

```
http://[surveillance server IP address or hostname]
```

If the Image Server (see page 139) has been configured with a port number other than the default port 80, you must specify the port number as well, separated from the IP address or hostname by a colon:

```
http://[surveillance server IP address or hostname]:[port number]
```

The content of the welcome page is managed through the Download Manager; therefore the welcome page will often look different across organizations.

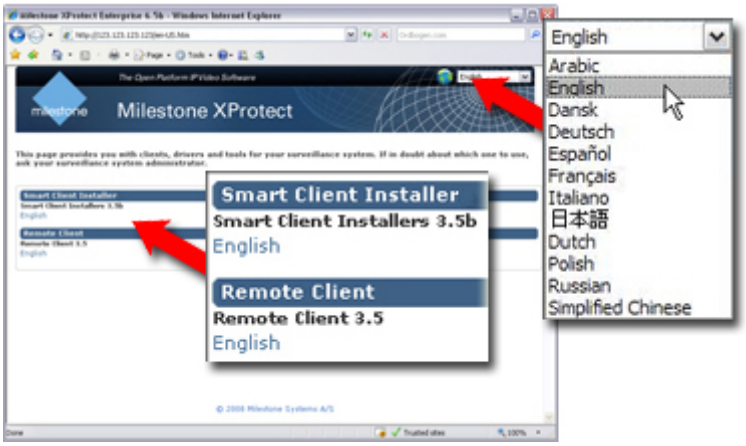
Initial Look

Immediately after you install XProtect Enterprise, the welcome page will provide access to two features: A Smart Client and a Remote Client in language versions matching the language version of your XProtect Enterprise system. Examples:

- If you have installed an English-language version of the XProtect Enterprise software, the two access clients will initially be in English.

- If you have installed a Japanese-language version of XProtect Enterprise, the two access clients will initially be in Japanese.

This initial look of the welcome page is automatically provided through the Download Manager's default configuration—for more information, see *Default Configuration of Download Manager* in the following. This example shows the welcome page as it looks immediately after installation of an English-language version of XProtect Enterprise:



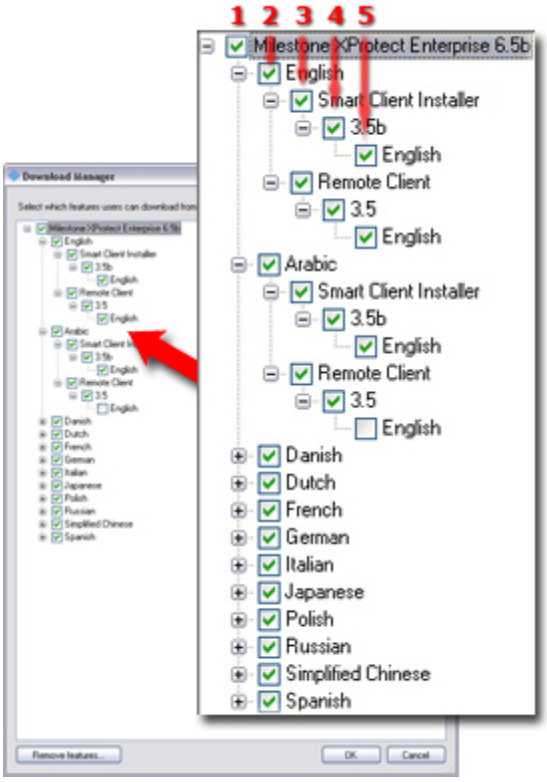
Welcome page from English-language version of XProtect Enterprise by default provides access to English-language versions of the Smart Client and Remote Client.

Download Manager's Default Configuration

The Download Manager has a default configuration. This ensures that your organization's users can access standard features without the surveillance system administrator having to set up anything.

The default configuration provides users with access to two features: A Smart Client and a Remote Client in language versions matching the language version of your XProtect Enterprise system.

The Download Manager's configuration is represented in a tree structure. With an English version of XProtect Enterprise, the tree would be structured as illustrated to the right.



Download Manager's Tree Structure

The **first level of the tree structure** (1 in the example illustration) simply indicates that you are working with an XProtect Enterprise system.

The **second level** (2) refers to the languages in which the welcome page is available. In the example, the welcome page is available in a dozen languages (English, Arabic, Danish, Dutch, French, etc.).

The **third level** (3) refers to the features which are—or can be made—available to users. In the example, these features are limited to the Smart Client and the Remote Client.

The **fourth level** (4) refers to particular versions of each feature, such as version 3.5, which are—or can be made—available to users.

The **fifth level** (5) refers to the language versions of the features which are—or can be made—available to users. In the example, only English versions are initially listed. This is because the example is from an English version of XProtect Enterprise; had you installed a Japanese version, only Japanese versions would initially be listed.

In the example, XProtect Enterprise has been installed an English-language version. If we expand one of the other languages in the tree structure's second level, for example Arabic, we will see that users who select the Arabic version of the welcome page will initially also only have access to English versions of the Smart Client and, potentially, the Remote Client.

The fact that only standard features are initially available—and only in the same language version as the surveillance system itself—helps reduce installation time and save space on the server. There is simply no need to have a feature or language version available on the server if nobody is going to use it.

You can, however, easily make more features and/or languages available as required. See the following for more information.

Making New Features Available

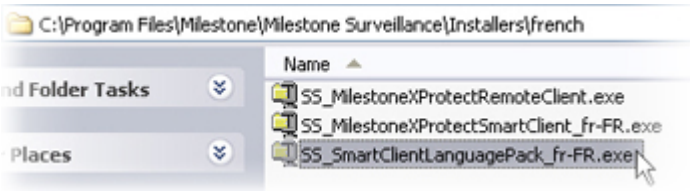
Making new features—including new language versions—available to your organization's users involves two procedures: First you install the required features on the surveillance system server. You then use the Download Manager to fine-tune which features should be available in the various language versions of the welcome page.

First: Installing New Features on Server

If the Download Manager is open, close it before installing new features on the server.

Installation files for Smart Client language versions, language packs, etc. are by default available on your surveillance system server in a folder called *Installers*. The *Installers* folder is located in the XProtect Enterprise installation folder, typically at C:\Program Files\Milestone\Milestone Surveillance\Installers.

To install a feature from the *Installers* folder, select the required language sub-folder, then double-click the required installation (.exe) file. In this example, we are about to install a French Smart Client language pack on the surveillance system server:



Tip: You can find more language versions of the Smart Client installer—and additional language packs—on the XProtect Enterprise software DVD as well as on www.milestonesys.com.

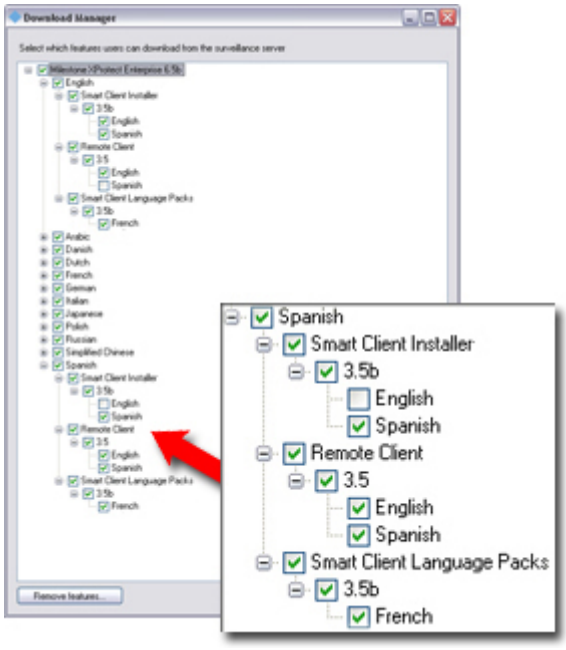
When a new feature has been installed on the surveillance system server, you will see a confirmation dialog. If required, you can open the Download Manager from the dialog.

Then: Making New Features Available through Download Manager

When you have installed new features—such as Smart Client language versions, language packs, etc.—they will by default be selected in the Download Manager, and thus immediately be available to users via the welcome page.

You can always show or hide features on the welcome page by selecting or clearing check boxes in the Download Manager's tree structure.

In this example, we have specified that users who select the Spanish-language version of the welcome page should have access to a Spanish version of the Smart Client, English and Spanish versions of the Remote Client, and a French language pack for the Smart Client:



Tip: You can change the sequence in which features and languages are displayed on the welcome page: In the Download manager's tree structure, simply drag items and drop them at the required position.

Hiding and Removing Features

You can remove features in several ways:

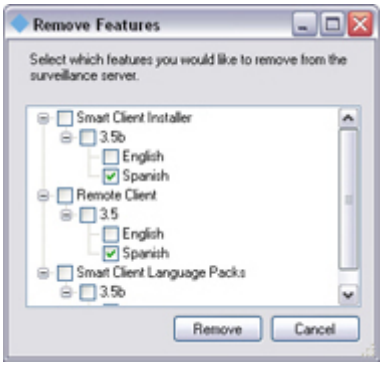
- You can **hide features** from the welcome page by clearing check boxes in the Download Manager's tree structure. In that case, the features will still be installed on the surveillance system server, and by selecting check boxes in the Download Manager's tree structure you can quickly make the features available again.

- You can **remove features** which have previously been made available through the Download Manager. This will remove the installation of the features on the surveillance system server. The features will disappear from the Download Manager, but installation files for the features will be kept in the surveillance system server's *Installers* folder, so you can re-install them later if required.

  1. In the Download Manager, click the *Remove features...* button.

  2. In the *Remove Features* window, select the features you want to remove. In the following example, we have selected to remove a Spanish Smart Client installer and a Spanish Remote Client.

  3. Click *OK*. You will be asked to confirm that you want to remove the selected features. If you are sure, click the *Yes* button.



- You can **remove installation files for non-required features** from the surveillance system server. This can help you save disk space on the server if you know that your

organization is not going to use certain features—typically non-relevant language versions. See Removing Installation files for End-User Features on page 189 for more information.

Virus Scanning

If you are using virus scanning software on the XProtect Enterprise server, it is likely that the virus scanning will use a considerable amount of system resources on scanning data from the Download Manager. If allowed in your organization, disable virus scanning on all or parts of the XProtect Enterprise server. For more information see Virus Scanning Information on page 162.

Logging

Various types of log files can be generated by XProtect Enterprise. Most log files generated by XProtect Enterprise use a shared structure complying with the W3C Extended Log File Format. Each log file consists of a header and a number of log lines:

- The *header* outlines the information contained in the log lines.
- The *log lines* consist of two main parts: the log information itself and an encrypted part. The encrypted part makes it possible—through decryption and comparison—to assert that a log file has not been tampered with.

Administrator Application Log Files

These files log activity in the *Administrator* application. A log file is created for each day the *Administrator* is used.

Administrator log files are by default placed in the folder containing the XProtect Enterprise software, typically C:\Program Files\Milestone\Milestone Surveillance\. Note, however, that the location as well as the number of days to log can be changed in the *General Settings* window's *Logfile Settings* section (see page 76).

Administrator log files are named according to the structure AdminYYYYMMDD.log, e.g. *Admin20070615.log*.

Recording Server Service Log Files

These files log activity in the R*ecording Server* (see page 68) when it runs as the *Milestone Recording Server* service. A log file is created for each day the service is used.

Milestone Recording Server service log files are by default placed in the folder containing the XProtect Enterprise software, typically C:\Program Files\Milestone\Milestone Surveillance\. Note, however, that the location as well as the number of days to log can be changed in the *General Settings* window's *Logfile Settings* section (see page 76).

Milestone Recording Server service log files are named according to the structure RecordingServerYYYYMMDD.log, e.g. *RecordingServer20070615.log*.

Event Log Files

These files log information about registered events (read more about events in *About Input, Events & Output ...* on page 84). A log file is created for each day on which events have occurred.

Event log files are by default placed in the folder containing the XProtect Enterprise software, typically C:\Program Files\Milestone\Milestone Surveillance\. Note, however, that the location as well as the number of days to log can be changed in the *General Settings* window's *Event Recording Settings* section (see page 76).

Event log files should be viewed using the *Smart Client* (see page 175) or the *Viewer* (see page 169):

- ***Smart Client*:** In the Browse tab's Alerts section, select the required event, then click the Get List button to see when the event in question was detected.
- ***Viewer:*** Select the *Viewer*'s Alarm Overview control panel, then click the *Events* button to view the events log.

Image Server Service Log Files

These files log activity on the *Image Server* service. A log file is created for each day the *Image Server* is used.

Image Server log files are by default placed in the folder containing the XProtect Enterprise software, typically C:\Program Files\Milestone\Milestone Surveillance\.

Image Server log files are named according to the structure ISLog_YYYYMMDD.log, e.g. *ISLog_20070615.log*.

Image Server Audit Log Files

These files log *Remote Client* (see page 178) and *Smart Client* (see page 175) user activity, if audit logging is enabled in the *Image Server Administrator* (see page 139). A log file is created for each day with remote user activity.

Image Server audit log files are by default placed in a subfolder named *ISAuditLog* under the folder containing the XProtect Enterprise software, typically C:\Program Files\Milestone\Milestone Surveillance\.

Image Server audit log files are named according to the structure is_auditYYYMMDD.log, e.g. *is_audit20070615.log*.

Image Import Service Log Files

These files log activity regarding the *Milestone Image Import* service, which is used for fetching pre-alarm images, and storing the fetched images in the database. Pre-alarm images is a feature available for selected cameras only; it enables sending of images from immediately before an event took place from the camera to the surveillance system via e-mail.

Image Import Service log files are by default placed in the folder containing the XProtect Enterprise software, typically C:\Program Files\Milestone\Milestone Surveillance\.

Image Import Service log files are named according to the structure ImageImportLog_YYYMMDD.log, e.g. *ImageImportLog20070615.log*.

Export Log Files

These files log activity regarding database export from the *Viewer (*see page 169). A log file is created for each day on which export was performed.

Export log files are by default, exported databases as well as the export log file are placed in an *Exported Images* folder on the desktop of the computer on which the export was performed. Note, however, that the export location may be changed as part of the export process.

Export log files are named according to the structure ExportYYYMMDD.log, e.g. *Export20070615.log*. Note, however, that database exports may be encrypted and/or compressed, in which case export log files are also encrypted/compressed and further file extensions, such as *.mzi* or *.men* may appear in export log file names.

Integrity Checks and Possible Error Messages

Log files are subjected to an integrity check once every 24 hours. The result of the integrity check is automatically written to a file named according to the structure LogCheck_YYYYMMDD.log, e.g. *LogCheck_20070615.log*. The log check file is by default placed in the folder containing the XProtect Enterprise software, typically C:\Program Files\Milestone\MilestoneSurveillance\.

Any inconsistencies will be reported in the form of error messages written in the log check file. The following table lists possible error messages (other, non-error, messages may also appear in the log check file):

Error Message	Description
"Log integrity information was not found. Log integrity can't be guaranteed."	The log file could not be checked for integrity.
"Log information does not match integrity information. Log integrity can't be guaranteed."	The log file exists, but does not contain the expected information. Thus, log integrity cannot be guaranteed.
"[Log file name] not found."	The log file was not present.
"[Log file name] is empty."	The log file was present, but empty.
"Last line changed/removed in [log file name]."	The last line of the log file did not match validation criteria.
"Encrypted data missing in [log file name] near line [#]."	The encrypted part of the log line in question was not present.
"Inconsistency found in [log file name] near line [#]."	The log line does not match the encrypted part.
"Inconsistency found in [log file name] at beginning of log file."	The log file header is not correct. This situation is most likely to occur if a user has attempted to delete the beginning of a log file.

Video Device Drivers

Updating Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to an XProtect Enterprise system. The XProtect Video Device Drivers should therefore be installed on your XProtect Enterprise system.

Video device drivers are installed automatically during the initial installation of your XProtect Enterprise system. However, new versions of XProtect Video Device Drivers are released and made available on the Milestone website, www.milestonesys.com, from time to time.

When updating your system's XProtect Video Device Drivers, it is recommended that you remove the old version of the drivers before installing the new version.

IMPORTANT: When you remove your XProtect Enterprise system's video device drivers, your system will not be able to communicate with camera devices until you have installed the new version of the video device drivers. It is therefore highly recommended that you perform the update of your XProtect Video Device Drivers at a time when you do not expect important incidents to take place.

Removing Old Version of Video Device Drivers

To remove XProtect Video Device Drivers prior to installing a later version of the drivers, use the following procedure on the XProtect Enterprise server(s) on which the XProtect Video Device Drivers are installed:

1. Open Windows' *Control Panel*, and select *Add or Remove Programs*. This will open the *Add or Remove Programs* window.

2. In the *Add or Remove Programs* window, select the *Video Device Driver Vx.x* entry (where *x.x* indicates the relevant version number), and click the *Remove* button.

3. You will be asked to confirm that you want to remove the XProtect Video Device Drivers. Click *OK* to remove the XProtect Video Device Drivers.

Installing New Version of Video Device Drivers

To begin installation of the new XProtect Video Device Drivers version, do the following:

1. On the XProtect Enterprise server(s) on which you want to install the new XProtect Video Device Drivers version, shut down any running Milestone software, including any running *Recording Server* service (see page 68).

2. Double-click the downloaded XProtect Video Device Driver file *DeviceInstaller.exe* to begin installation.

   Note: Depending on your security settings, one or more Windows security warnings may appear after you click the link. If such security warnings appear, accept security warnings by clicking *Run* or similar (exact button text depends on your browser version).

3. Select required language, and click *OK*. This will open the *Video Device Driver Setup Wizard*, which will guide you through the installation.

4. On the wizard's first step, click the *Next* button.

5. On the wizard's second step, an installation path is automatically suggested. Simply click *Next* to continue.

6. On the wizard's third step, select *Device drivers for Enterprise systems* from the menu, and click *Next*.

7. The wizard is now ready to install the video device drivers. Click the *Install* button to complete the installation of the video device drivers.

8. When ready, remember to start any stopped *Recording Server* service again (see page 68)

Virus Scanning Information

Virus scanning on the XProtect Enterprise server, and computers to which data is archived, should if possible be avoided:

- If you are using virus scanning software on the XProtect Enterprise server, or on a computer to which data is archived, it is likely that the virus scanning will use a considerable amount of system resources on scanning all the data which is being archived. This may affect system performance negatively. Also, virus scanning software may temporarily lock each file it scans, which may further impact system performance negatively.

- Likewise, virus scanning software on the XProtect Enterprise server is likely to use a considerable amount of system resources on scanning data used by the Download Manager.

If allowed in your organization, you should therefore disable any virus scanning of affected areas (such as camera databases, etc.) on the XProtect Enterprise server as well as on any archiving destinations.

Protecting Databases from Corruption

In the *Administrator* application's *Camera Settings for [Device Name] [Camera Name]* window (see page 43) you are able to select which action to take if a camera database becomes corrupted. The actions include several database repair options. While being able to select such actions is highly valuable, it is of course even better to take steps to ensure that your camera databases do not become corrupted:

Power Outages: Use a UPS

The single biggest reason for corrupt databases is the surveillance system server being shut down abruptly, without files being saved and without the operating system being closed down properly. This may happen due to power outages, due to somebody accidentally pulling out the server's power cable, or similar.

The best way of protecting your surveillance system server from being shut down abruptly is to equip your surveillance system server with a UPS (Uninterruptible Power Supply). The UPS works as a battery-driven secondary power source, providing the necessary power for saving open files and safely powering down your system in the event of power irregularities. UPSs vary in sophistication, but many UPSs include software for automatically saving open files, for alerting system administrators, etc.

Selecting the right type of UPS for your organization's environment is an individual process. When assessing your needs, however, do bear in mind the amount of runtime you will require the UPS to be able to provide if the power fails; saving open files and shutting down an operating system properly may take several minutes.

Windows Task Manager: Be Careful when Ending Processes

When working in Windows Task Manager, be careful not to end any processes which affect the surveillance system. If you end an application or system service by clicking *End Process* in the Windows Task Manager, the process in question will not be given the chance to save its state or data before it is terminated. This may in turn lead to corrupt camera databases.

Windows Task Manager will typically display a warning if you attempt to end a process. Unless you are absolutely sure that ending the process will not affect the surveillance system, make sure you click the *No* button when the warning message asks you if you really want to terminate the process.

Hard Disk Failures: Protect Your Drives

Hard disk drives are mechanical devices, and as such they are vulnerable to external factors. The following are examples of external factors which may damage hard disk drives and lead to corrupt camera databases:

- Vibration (make sure the surveillance system server and its surroundings are stable)
- Strong heat (make sure the server has adequate ventilation)

- Strong magnetic fields (avoid)
- Power outages (make sure you use a UPS; see more information in the previous)
- Static electricity (make sure you ground yourself if you are going to handle a hard disk drive).
- Fire, water, etc. (avoid)

Using 3 GB Operating System Virtual Memory

Microsoft Windows 32-bit operating systems can address 4 GB of virtual memory. The operating system kernel reserves 2 GB for itself, and each individual running process is allowed to address another 2 GB. This is Windows' default setting, and for the vast majority of XProtect Enterprise installations it works fine.

In XProtect Enterprise 6.5d or newer, the main components of the server—the Recording Server service and the Image Server service—have been compiled with the *LARGEADDRESSAWARE* flag. This means you can optimize the memory usage of XProtect Enterprise's Recording Server and Image Server services by configuring your 32-bit Windows operating system so that it restricts the kernel to 1GB of memory, leaving 3GB of address space for processes compiled with the *LARGE-ADDRESSAWARE* flag.

This should improve the stability of especially the Recording Server service by allowing it to exceed the previous 2 GB virtual memory limit, making it possible for it to use up to 3 GB of memory. The change in Windows configuration is known as *3 GB switching*.

When Is 3 GB Switching Relevant?

For very large XProtect Enterprise installations and/or for installations with many megapixel cameras it can be relevant to change Windows' settings so that only 1 GB of virtual memory is reserved for the operating system kernel, leaving 3 GB for running processes.

If using Windows' default setting, with only 2 GB virtual memory reserved for running processes, it has been seen that the Recording Server service in very large installations of XProtect Enterprise may:

- Behave erratically if getting very close to the 2 GB virtual memory limit. Symptoms can include database corruption, and client-server or camera-server communication errors.
- Become unstable and crash if exceeding the 2 GB virtual memory limit,. During such crashes, the code managing the surveillance system databases is not closed properly, and databases will become corrupt. In case of a crash, Windows will normally restart the Recording Server service. However, when the Recording Server service is restarted, one of its first tasks will be to repair the databases. The database repair process can in some cases take several hours, depending on the amount of data in the corrupted databases.

If you experience such problems, and you run XProtect Enterprise 6.5d or newer, making Windows use 3 GB for running processes is likely to solve the problems.

If you have not experienced such problems, but you run XProtect Enterprise 6.5d or newer and your XProtect Enterprise installation is very large and/or features many megapixel cameras, 3 GB switching is likely to help prevent the problems from occurring.

What to Do

The way to configure 32-bit Windows to be *LARGEADDRESSAWARE* depends on your type of Windows operating system. In the following, you will see to methods outlining Microsoft's recommended procedure for increasing the per-process memory limit to 3 GB. Use the first method

if running Windows XP Professional or Windows Server 2003. Use the second method if running Windows 2008 Server, Windows Vista Business, Windows Vista Enterprise or Windows Vista Ultimate.

If Running Windows XP Professional or Windows Server 2003

IMPORTANT: Improper modification of boot.ini can render the operating system inoperable. Milestone Systems do not assume any responsibility for changes you make to the operating system.

Adding the 3 GB Switch

The following technique can be used to add the 3 GB switch to the boot.ini file. From a command prompt, enter the following to add the 3 GB switch to the end of the first line of the operating system section in the boot.ini file (requires administrative privileges):

```
BOOTCFG /RAW "/3GB" /A /ID 1
```

Where

`/RAW` Specifies the operating system options for the boot entry. The previous operating system options will be modified.

`"/3GB"` Specifies the 3 GB switch.

`/A` Specifies that the operating system options entered with the /RAW switch will be appended to the existing operating system options.

`/ID` Specifies the boot entry ID in the OS Load Options section of the boot.ini file to add the operating system options to. The boot entry ID number can be obtained from performing the command: BOOTCFG /QUERY (this displays the contents of the boot.ini file) at the command prompt.

A reboot is required after editing the boot.ini file for the changes to take effect.

Removing the 3 GB Switch

If you want to undo the 3 GB switch mentioned above, follow this procedure:

Select *Start* > *Control Panel*, and double-click the *System* icon. Select the *Advanced* tab, and click the *Settings* button in the *Startup and Recovery* section. Click the *Edit* button in the *System Startup* section. The boot.ini file will launch in an editor. Remove the "/3GB" from the end of the appropriate boot entry line under the [operating systems] section. Save and close the file. Click *OK* in the *Startup and Recovery* section. A reboot is required after editing the boot.ini file for the changes to take effect.

If Running Windows 2008 Server or Windows Vista

IMPORTANT: Improper modification of the operating system boot entry can render the operating system inoperable. Milestone Systems do not assume any responsibility for changes you make to the operating system.

Adding the 3 GB Switch

Select *Start* > *All Programs* > *Accessories*, right-click *Command Prompt*, select *Run as …* administrator, then click *Continue*.

Enter the following command to add the 3 GB switch to the current operating system boot entry:

```
BCDEDIT /SET INCREASEUSERVA 3072
```

Where

`USERVA` Specifies an alternate amount of user-mode virtual address space for operating systems.

`3072` Specifies 3 GB (3072 MB).

A reboot is required after editing the boot configuration data store for the changes to take effect.

Removing the /3GB Switch

Select *Start* > *All Programs* > *Accessories*, right-click *Command Prompt*, select *Run as …* administrator, then click *Continue*.

Enter the following command to remove the 3 GB switch from the current operating system boot entry:

```
BCDEDIT /DELETEVALUE INCREASEUSERVA
```

A reboot is required after editing the boot configuration data store for the changes to take effect.

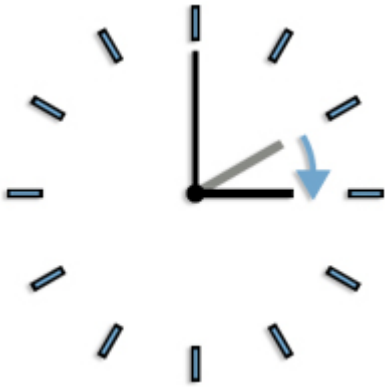
Daylight Saving Time

Daylight saving time (DST, also known as summer time) is the practice of advancing clocks in order for evenings to have more daylight and mornings to have less.

Typically, clocks are adjusted forward one hour sometime during the spring season and adjusted backward sometime during the fall season, hence the saying *spring forward, fall back*.

Note that use of DST varies between countries/regions.

When working with a surveillance system, which is inherently time-sensitive, it is important to know how the system handles DST.



Clocks are adjusted forward when DST starts

Spring: Switch from Standard Time to DST

The change from standard time to DST is not much of an issue since you jump one hour forward. Typically, the clock jumps forward from 02:00 standard time to 03:00 DST, and the day thus has 23 hours.

In that case, there is simply no data between 02:00 and 03:00 in the morning since that hour, for that day, did not exist.

Fall: Switch from DST to Standard Time

When you switch from DST to standard time in the fall, you jump one hour back. Typically, the clock jumps backward from 02:00 DST to 01:00 standard time, repeating that hour, and the day thus has 25 hours.

In that case, you will reach 01:59:59, then immediately revert back to 01:00:00. If the system did not react, it would essentially re-record that hour, so the first instance of, for example, 01:30 would be overwritten by the second instance of 01:30.

Because of this, XProtect Enterprise will forcefully archive (see page 125) the current video in the event that the system time changes by more than five minutes. The first instance of the 01:00 hour will not be viewable directly from access clients (Remote Client and Smart Client; see page 172). However, the data is recorded and safe, and it can be browsed using the Viewer application (see page 169) by opening the archived database directly.

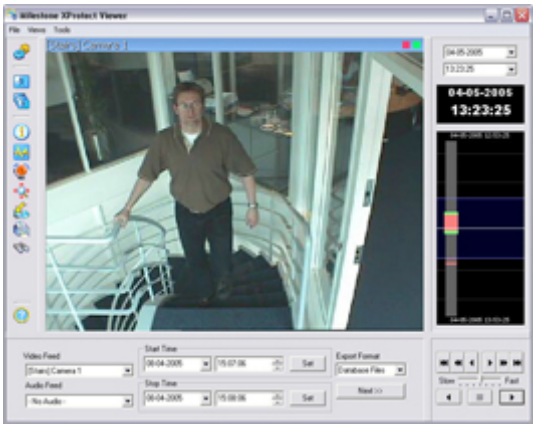
Viewer

The *Viewer* is a standalone application which lets you browse and play back video recordings. The *Viewer* also lets you print still images, send still images via e-mail, and export entire video and audio sequences in a variety of formats.

The *Viewer* can be accessed in two ways:

- ***If you work on the surveillance system server*:** On the surveillance system server, the *Viewer* is automatically installed as part of the XProtect Enterprise installation. You access the *Viewer* from Windows' *Start* menu: Select *Start* > *All Programs* > *Milestone XProtect Enterprise* > *Viewer*.

- ***By people who have received video evidence material from your surveillance system*:** This type of users are typically police officers, internal or external investigators, or similar. When Smart Client (see page 175) operators export video evidence, they are able to include the *Viewer* with the exported evidence. This is a great advantage for the recipient of the exported evidence, since no installation is required in order to use the *Viewer* for browsing exported evidence.



The *Viewer*: In this example, the *Viewer* displays video from a single camera; the Viewer can display video from several cameras simultaneously. Note that content of the *Viewer*'s toolbar may vary depending on configuration.

Where can I find more information about the *Viewer*? The *Viewer* has its own built-in help system. Alternatively, refer to the *Viewer* User's Manual, available on the XProtect Enterprise software DVD as well as from www.milestonesys.com.

Monitor

Where Is the Monitor Application?

If you have used previous versions of XProtect Enterprise, you may note that the *Monitor* application for viewing of live video on the surveillance system server itself has been discontinued as from XProtect Enterprise version 6.5.

When you want to view live video, use a Smart Client (see page 175). The Smart Client has features for viewing live video which are far superior to those previously available in the *Monitor* application.

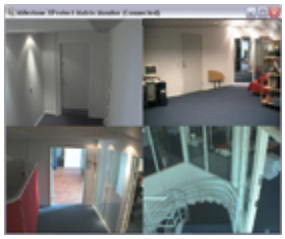
Tip: A Smart Client is automatically installed on the surveillance system server as part of the XProtect Enterprise installation.

Tip: The *Monitor* application also included the so-called *Viewer* application for browsing recorded video. The *Viewer* is still available, although we recommend the Smart Client for browsing recorded video. If you want to use the *Viewer* (see page 169), access it from Windows' *Start* menu: Select *Start* > *All Programs* > *Milestone XProtect Enterprise* > *Viewer*.

Matrix Monitor

Milestone XProtect Matrix is an integrated product allowing distributed viewing of video from any camera on any monitor on a network operating with XProtect Enterprise.

A computer on which Matrix-triggered video can be shown is known as a Matrix recipient. Being able to view Matrix-triggered video requires that either the *Matrix Monitor* application or a *Smart Client* (see page 175) is installed on the Matrix recipient computer.



Example: Viewing video in the *Matrix Monitor* application

There are two ways in which Matrix-triggered video can appear on a Matrix recipient:

- Another user wants to share important video, and sends it from the surveillance system's *Monitor* application, from a *Smart Client* (see page 175), or from a custom-made web page to the required Matrix recipient

- The video is sent to the required Matrix recipient automatically when a predefined event occurs; for example when a door sensor detects that a door is opened, or when the surveillance system detects motion in the video from a camera

As part of the video exchange between computers on the XProtect Enterprise/Matrix system, other computers (exactly which computers are defined as part of the Matrix configuration) are able to send commands to Matrix recipients. The commands typically tell the Matrix recipient to connect to, or disconnect, video feeds from a particular cameras.

Where can I find more information about the Matrix Monitor? Refer to the Matrix Monitor User's Manual, available on the XProtect Enterprise software DVD as well as from www.milestonesys.com.

Access Clients

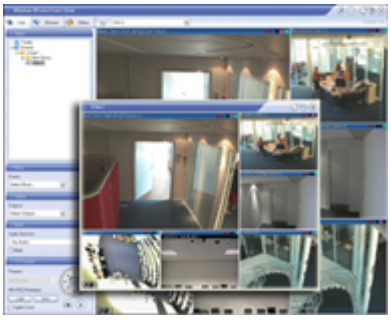
Access Client Overview

Remote users can access an XProtect Enterprise surveillance system in different ways:

- With a Remote Client – see page 178 (run straight from server, good selection of standard features)

Example of Remote Client

- With a Smart Client – see page 175 (installed locally, very feature-rich, based on the .NET platform and thus highly flexible for future integration of plugins, etc.)



Example of Smart Client

- With a PDA Client (see page 179) installed on a handheld computer device with a wireless connection

Example of PDA Client

The way remote access is handled at the surveillance system server end is different, depending on remote access method:

Providing Access through a Remote Client or Smart Client

Surveillance system administrators use two administration tools for providing access through the Remote Client and Smart Client: The Image Server and the Download Manager:

- **Image Server:** Recordings viewed by Remote Client and Smart Client users are provided by the XProtect Enterprise surveillance system's Image Server. The Image Server runs as a service on the XProtect Enterprise server; it does not require separate hardware. The surveillance system administrator uses the *Image Server Administrator* window (see page 139) to manage Remote Client and Smart Client access to the surveillance system.

- **Download Manager:** In order to get hold of a Remote Client or Smart Client, users connect to the surveillance system server which will present them with a welcome page. The welcome page will list the available clients and language versions. The system administrator uses the Download Manager (see page 152) to control which clients and language versions should be available to users on the welcome page.

Providing Access through a PDA Client

Use of the PDA Client requires that a matching PDA Server (see page 179 is installed on the surveillance system. The PDA Server is installed on an Internet Information Services (IIS) server, and is used as a front-end to the XProtect Enterprise system's Image Server, on which user rights are defined. The PDA Server handles login and session requests between the PDA Client and the Image Server. The PDA Server also handles resizing of surveillance video to fit the screen layout of the PDA Client. For more information, see Installing & Configuring the PDA Server on page 180 as well as the description of the *Image Server Administrator* window (see page 139).

Deciding Which Access Client to Use

When deciding which access client solution is the best choice for your organization, you may find it helpful to review the following.

Note: Systems and requirements differ from organization to organization. The following questions and answers are thus for guidance only.

Do you require a handheld solution?

- **Yes:** Use the PDA Client/Server solution. If required, you can of course combine the PDA solution with other remote access solutions, such as the Smart Client.
- **No:** Determine your needs based on the questions and answers provided in the following.

Is it acceptable to install client software on remote users' computers?

- **Yes:** Use the Smart Client (see page 175).
- **No:** Use the Remote Client (see page 178); remote users run the Remote Client straight from the XProtect Enterprise server.

Will you require a large amount of future flexibility from your remote access solution?

- **Yes:** Use the Smart Client. Due to the way the software has been developed, the Smart Client offers a high degree of flexibility for integration of new features, plugins, etc.
- **No:** Use the Remote Client.

Do you require a very feature-rich client application?

- **Yes:** Use the Smart Client. The Smart Client offers considerably more features for remote users than the other solutions.
- **No:** Use the Remote Client.

Do you require a large amount of flexibility re. remote users' ability to export data?

- **Yes:** Use the Smart Client. The Smart Client offers the ability to—individual user rights permitting—export evidence in the AVI (movie clip), JPEG (still image) as well as XProtect Enterprise database formats.
- **No:** Use the Remote Client. The Remote Client offers the ability to—individual user rights permitting—export evidence in the AVI and JPEG formats.

Will you use a .NET-based client application?

- **Yes:** Use the Smart Client. The .NET-based Smart Client offers more features for remote users than the other solutions. .NET Framework 2.0, downloadable from http://www.microsoft.com/downloads/, is required on computers running the Smart Client.
- **No:** Use the Remote Client. The Remote Client is not a .NET-based solution.

What is .NET? The. Net software development platform allows the interconnection of computers and services for the exchange and combination of data and objects. The platform makes extensive use of so-called web services, which provide the ability to use the web rather than single applications for various services. This in turn provides the ability for centralized data storage as well as automated updating and synchronization of information. The .NET platform enhances software developers' ability to create re-usable and customizable modules, which makes it possible to develop highly flexible software solutions. You can therefore, as a rule of thumb, expect .NET-based software to be highly flexible, ready for integration of new features, plugins, etc. However, organizations and their requirements are different, and some organizations find that the high degree of interconnection of services and computers inherent in a .NET-based solution is not desirable. Instead, such organizations rely on more classic Windows solutions.

Differences between Remote Client and Smart Client

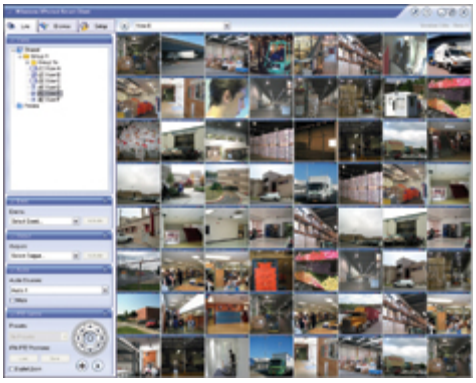
The following table outlines the main differences between the two non-PDA solutions, i.e. the Remote Client and Smart Client:

The Two Access Clients at a Glance	Remote Client	Smart Client
Remote User's Installation	None; the client is accessed from server through a browser.	Client must be installed on remote user's computer. .NET Framework is required on computers running the Smart Client.
Remote User's Feature Set	A good set of standard features.	Very feature-rich.
Remote User's Ease of Use	Very easy to use. Setup of views can be handled locally as well as centrally. With central views handling, users can begin using their clients instantly upon first login.	
System Administrator's Installation	The Image Server and Download Manager runs as automatically installed services on the XProtect Enterprise server. Only if clients are required in other languages than the XProtect Enterprise server itself is additional installation required.	

The Two Access Clients at a Glance	Remote Client	Smart Client
System Administrator's Feature Set	Very flexible; configuration through the *ImageServer Administrator* and Download Manager includes master-slaves handling, handling of local IP address ranges, language versions, etc.	
System Administrator's Access Control Options	Very flexible; choice of creating dedicated user accounts or importing users and groups of users from Active Directory; rights for accessing individual client and camera features can be determined on a per-user or per-group basis.	
Client Flexibility re. Future Features and Plugins	Limited.	.NET-based, thus offering a high degree of flexibility for integration of new features, plugins, etc.
Recommended Use	Systems on which installation of client software is not desirable. Systems on which a .NET client solution is not desirable. Systems on which the Active Directory support lets you leverage existing user accounts.	Systems on which a high degree of flexibility, e.g. use of remote access plugin features, will be required. Systems on which a .NET client solution is desirable. Systems on which the Active Directory support lets you leverage existing user accounts.

Smart Client

In the following, the Smart Client is briefly introduced. For detailed information about the Smart Client, see the Milestone XProtect Smart Client User's Manual, available on the XProtect Enterprise software DVD as well as from www.milestonesys.com. Once installed, the Smart Client also has its own built-in help system



The Smart Client provides users with extremely feature-rich access to the surveillance system. The Smart Client must be installed locally on the user's computer. See system requirements for the Smart Client under System Requirements on page 16.

Installation Options

The Smart Client can be installed in three ways:

- Download and Install the Smart Client from the surveillance system server (see page 176)

- Install the Smart Client from the XProtect Enterprise software DVD (see page 176)
- Silent Installation (Surveillance System Administrators Only) (see page 177)

Download and Installation from Server

Note: Surveillance system administrators automatically get a Smart Client installed on the surveillance system server; this happens as part of the surveillance system server installation.

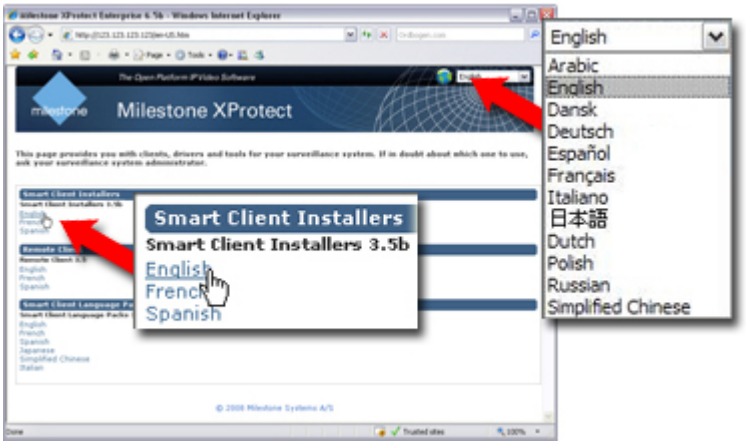
Typically, you download the Smart Client from the surveillance system server, and then install it on your computer. Alternatively, your surveillance system administrator may ask you to install the Smart Client from a DVD (see Installation from DVD on page 176).

To download and install the Smart Client from the surveillance system server, do the following:

1. Verify that your computer meets the Smart Client's minimum system requirements (see page 16).

2. Open an Internet Explorer browser (version 6.0 or later), and connect to the surveillance system server at the URL or IP address specified by your system administrator. When you are connected to the surveillance system server, you will see a welcome page.

3. On the welcome page, select your required language in the menu in the top right corner. Then go to the welcome page's *Smart Client Installers* section, and click the required Smart Client language version link.



Example: Selecting welcome page language and required Smart Client language version. Number of available languages may be different in your organization.

4. Depending on your security settings, you may receive one or more security warnings (*Do you want to run or save this file?*, *Do you want to run this software?* or similar; exact wording depends on your browser version). When this is the case, accept the security warnings (by clicking *Run* or similar; exact button names depend on your browser version).

5. The *Smart Client Setup Wizard* begins. In the wizard, click *Next*, and follow the installation instructions.

Installation from DVD

Typically, you download the Smart Client from the surveillance system server, then install it on your computer (see Download and Installation from Server on page 176). Alternatively, your surveillance system administrator may ask you to install the Smart Client from a DVD:

1. Verify that your computer meets the Smart Client's minimum system requirements.

2. Insert the surveillance system software DVD, wait for a short while, select required language, then click the *Install Milestone XProtect Smart Client* link.

   Tip: Depending on your security settings, you may receive one or more security warnings (*Do you want to run or save this file?*, *Do you want to run this software?* or similar; exact wording depends on your browser version). When this is the case, accept the security warnings (by clicking *Run* or similar; exact button names depend on your browser version).

3. When the installation wizard starts, click *Next* to continue the installation and follow the steps in the installation wizard.

Silent Installation

For surveillance system administrators, it is possible to deploy the Smart Client to users' computers using tools such as Microsoft Systems Management Server (SMS). Such tools let administrators build up databases of hardware and software on local networks. The databases can then—among other things—be used for distributing and installing software applications, such as the Smart Client, over local networks.

1. Locate the self-extracting Smart Client installation (.exe) file.

   You find the file in a subfolder under the folder *httpdocs*. The *httpdocs* folder is located under the folder in which your Milestone surveillance software is installed.

   The path would thus typically be C:\Program Files\Milestone\Milestone Surveillance\httpdocs\Smart Client Installers\[version number]\[language]\[language code].

   For example, an English-language version of the Smart Client installation file could be located at C:\Program Files\Milestone\Milestone Surveillance\httpdocs\Smart Client Installers\3.5b\English\en-US).

2. With an extraction tool, such as WinZip® or similar, extract the files contained in the installation file to a folder of your choice.

   When extraction is done, the folder to which you extracted will contain a small number of files, among these a file with the extension *.msi*. The .msi file is a Microsoft Windows Installer installation package covering the complete Smart Client installation procedure.

3. You can now use your systems management tool to deploy the .msi file.

   Alternatively, you can simply copy the msi. file to required computers, and run the .msi file from a command prompt. Examples:

   ```
   C:\Documents and Settings\you>msiexec /i "C:\folder_to_which_file_was_
   copied\SmartClientInstaller.msi" /quiet
   ```

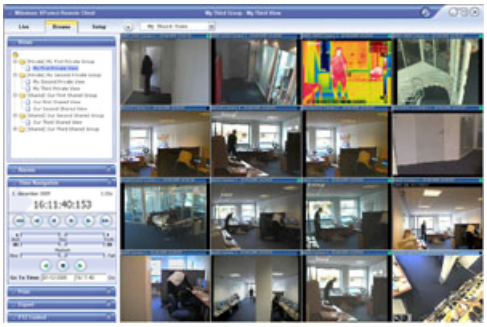
   where *msiexec* calls the Windows Installer, the parameter */i* indicates that you want to install, and the parameter */quiet* indicates a silent installation.

   On the target computer, the Smart Client is by default installed in C:\Program Files\Milestone\Milestone Smart Client. With the *TARGETDIR* property, you are able to specify a different installation folder. Example:

   ```
   C:\Documents and Settings\you>msiexec /I "C:\folder_to_which_file_was_
   copied\SmartClientInstaller.msi" /quiet TARGETDIR=C:\required_
   installation_folder\
   ```

Remote Client

In the following, the Remote Client is briefly introduced. For detailed information about the Remote Client, see the Milestone XProtect Remote Client User's Manual, available on the XProtect Enterprise software DVD as well as from www.milestonesys.com.



The Remote Client provides remote users with feature-rich access to the surveillance system. It lets users access multiple servers at a time, allowing remote user access across systems.

The Remote Client does not offer nearly as many features as the Smart Client (see page 175). However, the Remote Client is accessed through a browser and run straight from the XProtect Enterprise server. This eliminates the need for installing any client software. See system requirements for the Remote Client under System Requirements on page 16.

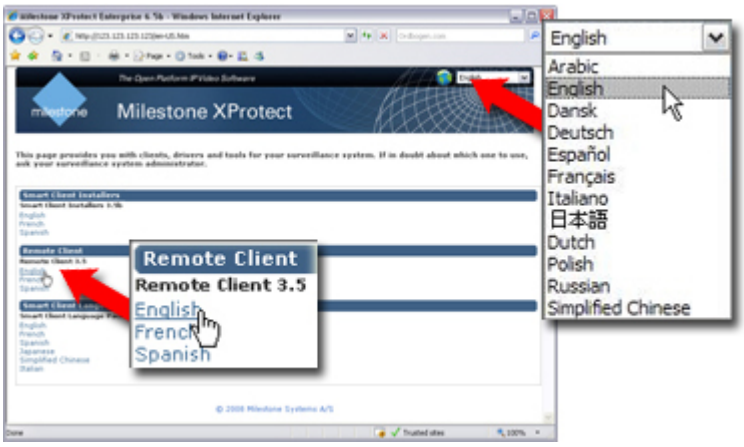
Accessing a Remote Client

The Remote Client is run directly from the XProtect Enterprise server; you simply access it through a browser:

1. Open an Internet Explorer browser (version 6.0 or later), and connect to the surveillance system server at the URL or IP address specified by your system administrator. When you connect to the XProtect Enterprise server, you will see a welcome page.

   If using Windows Vista, the Remote Client must be added as a trusted site in your browser (from your browser's *Tools* menu, select *Internet Options* > *Security* > *Trusted sites*).

2. On the welcome page, select your required language in the menu in the top right corner. Then go to the welcome page's *Remote Client* section, and click the required Remote Client language version link.



Example: Selecting welcome page language and required Remote Client language version. Number of available languages may be different in your organization.

3. Specify your login information in the following fields:

   - ***Previous Logins*: *Only available if you have logged in before.*** Lets you reuse previously specified login details (except any password, which you must always type yourself). This can greatly speed up the login process.

- ***Address:*** Type the URL or IP address of the surveillance system server, as specified by your system administrator.
- ***Port:*** Internet connections may use different ports for different purposes. Specify the port number, your system administrator has asked you to use when logging in to the Remote Client. In most circumstances, port 80 is used.
- ***Authentication*:** Select between different methods of authentication (i.e. the process of verifying that you are who you claim you are). Consult your surveillance system administrator if in doubt about which authentication method to use.
    - *Windows (current user)*, with which you will be authenticated through your current Windows login, and do not have to specify any user name or password. This is the default authentication method, i.e. the method which is automatically used unless you select another method.
    - *Windows*, with which you will be authenticated through your Windows login, but you will need to type your Windows user name and password.
    - *Basic*, with which you will be authenticated through a user/password combination defined on the surveillance system server.
- ***Username*:** Type your user name as specified by your system administrator. The user name is case-sensitive, i.e. there is a difference between typing, for example, *amanda* and *Amanda*.
- ***Password*:** Type your password as specified by your system administrator. The password is case-sensitive.

4. Click the *Login* link.

PDA Client & Server

The following primarily covers installation and configuration of the PDA Server front-end to the XProtect Enterprise system's Image Server. For detailed information about using the PDA Client, see the Milestone XProtect PDA Client User's Manual, available on the XProtect Enterprise software DVD as well as from www.milestonesys.com.

The PDA Client and PDA Server applications enable remote access to the XProtect Enterprise surveillance system via a PDA (Personal Digital Assistant; a handheld computer device) with a wireless connection. Handheld remote access can be highly valuable in many situations. For example, first responders to break-ins, fires, etc. will be able to view live as well as recorded video of the incidents while on their way to the incidents (wireless connection permitting).

The ***PDA Server*** is installed on an Internet Information Services (IIS) server, and is used as a front-end to the XProtect Enterprise system's Image Server. The PDA Server handles login and session requests between the PDA Client and the Image Server. The PDA Server also handles resizing of surveillance video to fit the screen layout of the PDA Client.

The ***PDA Client*** is used for viewing live and recorded video from the XProtect Enterprise surveillance system on the PDA.

PDA Server Installation & Configuration Procedure

Note: The PDA Server does not support Windows authentication. When using the Image Server Administrator (see page 139) for defining users with access through the PDA Server/PDA Client solution, make sure you add the users with the authentication method *basic authentication*.

Before the PDA Server can be installed on a server, Internet Information Services (IIS) and Microsoft .NET Framework 2.0 (version 2.0.50727) must be installed and configured on the server.

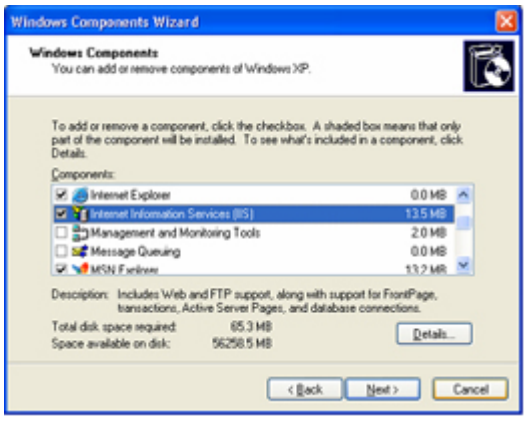
Installing IIS and .NET Framework

To Install IIS and .NET Framework on the server, do the following:

First: IIS Installation

Note: The following procedure describes IIS installation on Windows XP. If you are using Windows 2000 Server or Windows 2003 Server, IIS and .NET Framework are normally installed during the installation of the operating system.

1. In Windows' *Start* menu, select *Control Panel*, then *Add or Remove Programs*.
2. In the left part of the *Add or Remove Programs* dialog, click *Add/Remove Windows Components*. This will open the *Windows Components Wizard*.
3. In the wizard's *Components* list, select *Internet Information Services (IIS)* and click *Next*:


Windows Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Internet Explorer 0.0 MB
Internet Information Services (IIS) 13.5 MB
Management and Monitoring Tools 2.0 MB
Message Queuing 0.0 MB
Description: Includes Web and FTP support, along with support for FrontPage, transactions, Active Server Pages, and database connections.
Total disk space required: 65.3 MB
Space available on disk: 56258.5 MB
Details...
< Back
Next >
Cancel

4. Follow the wizard's instructions to complete the installation.

Then: . NET Framework Verification

.NET Framework version 2.0 must be installed on the server in order to be able to run the *PDA Server*.

Note that later versions of. Net Framework may also be present on the server. If .NET Framework 2.0 *as well as* one or more later versions are present on the server, Windows' default settings may cause a later .NET Framework version to be used instead of .NET Framework 2.0. To verify/change which .NET Framework version is used, do the following:

1. Click *Start*, and select *Control Panel*.
2. Click *Administrative Tools*.
3. Click *Internet Information Services*.

4. In the *Internet Information Services* window's left pane, locate and right-click the *Default Web Site* item:

Example only; content on your server may be different

5. In the resulting menu, select *Properties*. This will open the *Default Web Site Properties* dialog.

6. Select the dialog's *ASP.NET* tab. The .NET Framework version in use will be indicated in the *ASP.NET version* field.

7. If required, change the *ASP.NET version* to *2.0.50727*.

8. Click *OK*.

9. Close the *Internet Information Services* and *Administrative Tools* windows if still open.

.NET Framework Registration

When IIS and .NET Framework are installed, you must register .NET Framework in the IIS:

1. In Windows' *Start* menu, select *Run...*.

2. In the *Open* field, type *C:\WINDOWS\Framework\v2.0.50727\aspnet_regiis.exe -i*

   Note that if you also have later .NET versions installed, you may have to type a slightly different path: *C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -i*

   Note: In both cases, make sure you include the *-i* parameter.

3. Click *OK* to register the .NET Framework in IIS.

Allowing Use of .NET Framework (Windows 2003 Only)

When .NET Framework is installed, you must allow use of .NET Framework by doing the following:

1. Click *Start*, and select *Control Panel*.

2. Click *Administrative Tools*.

3. Click *Internet Information Services*.

4. In the *Internet Information Services Manager*'s left pane, select the *Web Service Extensions* item.

5. On the *Extended* tab in the *Internet Information Services Manager*'s right pane, select *ASP.NET v2.0.50727*, and click the *Allow* button.

Tip: When IIS and .NET Framework have been installed and registered, it is a good idea to use Windows Update to check for, and download, any new service packs or security packs.

Installing the PDA Server

To Install the PDA Server, do the following:

Note: The following procedures describe installation of the PDA Server as the only application using IIS on the server, and with its default settings. If IIS is also used for other applications, it is recommended that you consult an experienced IIS administrator prior to installing the *PDA Server*.

First: IIS Port Configuration

Before you begin installing the *PDA Server*, you must configure IIS to use the port number on which the PDA Server is going to run:

1. In Windows' *Start* menu, select *Run...*.

2. In the *Open* field, type *inetmgr.exe* and click *OK*. This will display the *Internet Information Services* dialog.

3. In the left part of the dialog, expand the *computer* item until you see the *Default Web Site* item:

Example only; details enlarged for clarity; computer name is likely to be different on your server

4. Right-click the *Default Web Site* item, and select *Properties*. This will open the *Default Web Site Properties* dialog.

5. On the dialog's *Web Site* tab, set the *TCP Port* number to the number that *PDA Server* is going to use (the default port for the *PDA Server* is 8080), then click *OK*.

6. Back in the *Internet Information Services* dialog, verify that IIS is running. If IIS is not running, start IIS by right-clicking the *Default Web Site* item, then selecting *Start*.

Then: PDA Server Installation

Having configured the IIS port number, you are ready to begin installation of the *PDA Server* itself:

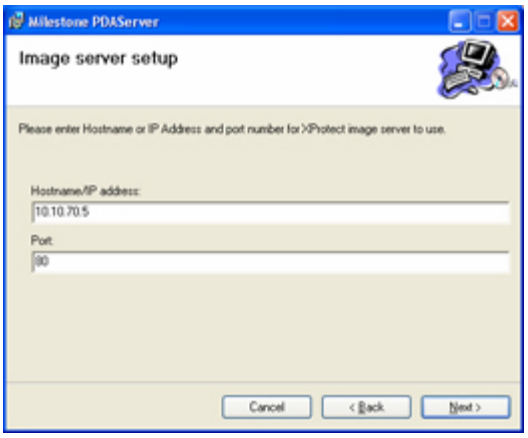
1. On the server, insert the XProtect Enterprise software DVD, wait for a short while, select required language, then click the *Install Milestone XProtect PDA Server* link.

   Alternatively, if you are installing a version downloaded from the internet, run the PDA Server installation file *PDAServerInstaller_[required language].exe* from the location you have saved it to.

   Tip: Depending on your security settings, you may receive one or more security

warnings (*Do you want to run or save this file?*, *Do you want to run this software?*). When this is the case, click the *Run* button.

2. Read and accept the license agreement. This will take you to the *Image server setup* step.

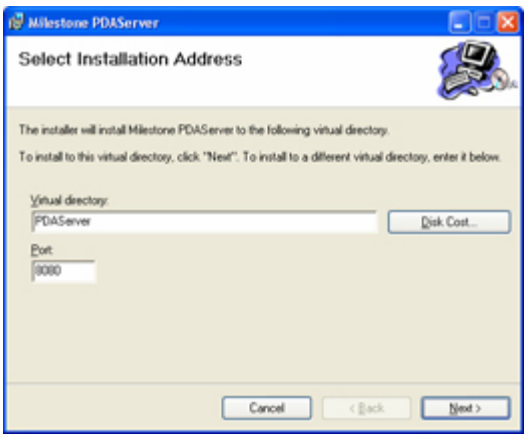


3. In the *Hostname/IP Address* field, specify the IP address or host name of the XProtect Enterprise server to which the *PDA Server* should connect.

Tip: If installing the *PDA Server* on the same server as the surveillance system itself, simply specify *Localhost*. If the PDA Server should connect to a master/slave system, specify the IP address or host name of the master server.

In the *Port* field, specify the port number used by the surveillance system's Image Server (default is port 80), then click *Next.*

4. An *Important Note* is displayed; it is highly recommended that you read it. When ready, click *Next*. This will take you to the *Select Installation Address* step.


Milestone PDAServer
Select Installation Address
The installer will install Milestone PDAServer to the following virtual directory.
To install to this virtual directory, click "Next". To install to a different virtual directory, enter it below.
Virtual directory:
PDAServer
Disk Cost...
Port:
8080
Cancel
< Back
Next >

5. In the *Virtual directory* field, specify the virtual directory in which the PDA Server should be installed on the IIS (default virtual directory is *PDA Server*).

In the *Port* field, specify the port number you used during IIS configuration (default port number is 8080).

6. Click *Next* twice.

7. When installation is completed, click the *Close* button.

Verifying the PDA Server Installation

Before you begin installing and using the PDA Client, it is highly recommended that you verify that the *PDA Server* is installed correctly: First make sure that the XProtect Enterprise system's *Recording Server* service and Image Server service are running, and that a user with access to relevant cameras has been set up in the *Image Server Administrator.*

Tip: You can use a *Remote Client* or *Smart Client* to verify that the Image Server's user setup works.

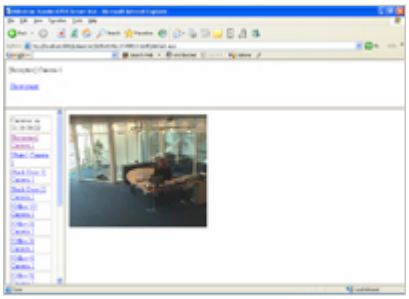
Then do the following:

1. Double-click the *PDA Server* desktop shortcut created during the *PDA Server* installation. This will open the *PDA Server Administrator* dialog:

2. In the lower half of the *PDA Server Administrator* dialog, verify that the *Test enabled* check box is selected, then click the link below the check box to open the test interface in a browser.

3. Log in to the test interface by typing the user name and password as set up on the *Image Server*, then click the *Login* button. The test interface will now log in to the *Image Server*, and list all cameras to which the user has access.

4. Click one of the camera links in the test interface's left frame. If an image (the latest recorded image from the selected camera) is displayed, the PDA Server is installed correctly.



PDA Server Installation Troubleshooting

The following issues may occasionally occur during or upon installation of the PDA Server. For each issue, one or more solutions are available.

PDA Server Cannot Be Installed

Solutions:

- Make sure that IIS is installed.
- Make sure that IIS is set up to use the correct port (default is port 8080), and that the same port number was used when the virtual directory was specified.
- Make sure that IIS is running.

Test Interface Cannot Be Displayed

Solutions:

- Make sure that the .NET Framework is registered on the IIS.
- Make sure that IIS is running.

Test Interface Is Displayed, but It Is Not Possible to Log In

Solutions:

- Start the *PDA Server Administrator* from the desktop shortcut, and verify that the IP address or hostname in the *Host/IP* field points to your Image Server. Also make sure that the port number in the *Port* field matches the port number on which the Image Server service is running.
- Make sure that the Image Server service is running on the surveillance system.

Make sure that the user account used when accessing the test interface has been correctly set up on the Image Server, and that the user account provides access to the required cameras.

Removal

Removing the Entire Surveillance System

What Will Happen to Recordings when I Remove the Surveillance Software?

Your recordings will not be removed; they will remain on the server even after the server software has been removed. Likewise, the XProtect Enterprise configuration file will remain on the server; this allows you to reuse your configuration if you later install XProtect Enterprise again.

To remove the entire XProtect Enterprise surveillance system (i.e. the surveillance server software and related installation files, the video device drivers, the Download Manager, the Viewer and the Smart Client) from your server, do the following:

1. Shut down all XProtect Enterprise components.
2. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*.
3. In the *Add or Remove Programs* window's list of currently installed programs, select the *Milestone XProtect Enterprise* ***system*** entry (not the *Milestone XProtect Enterprise* entry) and click the *Change/Remove* button.
4. The setup wizard appears; click the *Next* button, then the *Remove* button.
5. Select *Remove entire surveillance system*, then click *Next*, and complete the wizard's remaining steps.

Tip: If you have used the PDA Client/PDA Server solution, you may also want to remove the PDA Server software from the server (see page 187).

Removing Individual Components

Removing the Surveillance Server Software

To remove the XProtect Enterprise server software (including the Viewer, but no other surveillance system components, such as the Download Manager or the Smart Client), do the following:

1. Shut down all XProtect Enterprise components.
2. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*.
3. In the *Add or Remove Programs* window's list of currently installed programs, select the *Milestone XProtect Enterprise* entry (not the *Milestone XProtect Enterprise* ***system*** entry) and click the *Remove* button.
4. You will be asked to confirm that you want to remove XProtect Enterprise. If you are sure that you want to remove the software, click *OK*.
   - If a *Status Information* window appears on your screen during installation, simply click its *OK* button (the window simply provides a summary of what has been removed).

5. Click *Finish*.

Removing Video Device Drivers

Video device drivers are small programs used for controlling/communicating with the camera devices connected to an XProtect Enterprise system. To remove the video device drivers, do the following:

1. Open Windows' *Control Panel*, and select *Add or Remove Programs*.
2. In the *Add or Remove Programs* window, select the *Video Device Pack Vx.x* entry (where *x.x* indicates the relevant version number), and click the *Remove* button.
3. You will be asked to confirm that you want to remove the XProtect Video Device Drivers. Click *OK* to remove the XProtect Video Device Drivers.

Removing the Download Manager

The Download Manager (see page 152) is removed separately from the XProtect Enterprise software:

1. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*.
2. In the *Add or Remove Programs* window's list of currently installed programs, select *Milestone XProtect Download Manager*.
3. Click the *Remove* button.

Removing the Viewer

You cannot remove the Viewer separately; the Viewer is removed as part of the surveillance server software removal (see page 186).

Removing the Smart Client

To remove a Smart Client, do the following on the computer on which the Smart Client is installed:

1. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*.
2. In the *Add or Remove Programs* window's list of currently installed programs, select *Milestone XProtect Smart Client x.x* (where x.x refers to the version number).
3. Click the *Remove* button, and follow the removal instructions.

Removing the PDA Software

To remove the *PDA Server* and *PDA Client* software, use the following procedures:

PDA Server Removal Procedure

1. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*.

2. In the *Add or Remove Programs* window's list of currently installed programs, select the *Milestone PDA Server*.

3. Click the *Remove* button, and follow the removal instructions.

PDA Client Removal Procedure

The *PDA Client* may be removed in two ways: either directly from the PDA, or from a PC with ActiveSync.

Removing the PDA Client Directly from the PDA

1. Tap the PDA's *Start* button.

2. Select *Settings*.

3. Select the *System* tab.

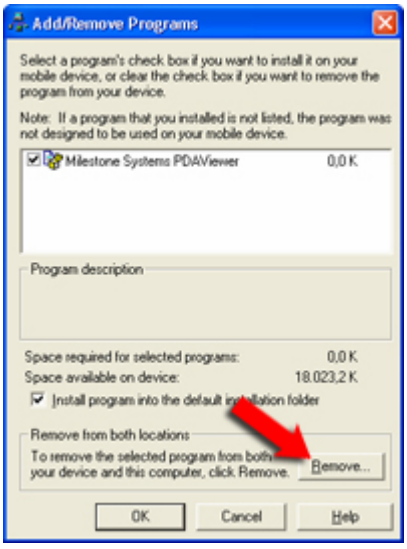
4. Select *Remove Programs*.

5. Select the *Milestone Systems PDA Client*, and tap the *Remove* button.

6. Select *Yes* when asked if you want to remove the program.

Removing the PDA Client from a PC with ActiveSync

Note: This method requires that the *PDA Client* was installed on the PC and transferred to the PDA through ActiveSync.


Add/Remove Programs
Select a program's check box if you want to install it on your mobile device, or clear the check box if you want to remove the program from your device.
Note: If a program that you installed is not listed, the program was not designed to be used on your mobile device.
Milestone Systems PDAViewer
0,0 K
Program description
Space required for selected programs:
0,0 K
Space available on device:
18.023,2 K
Install program into the default installation folder
Remove from both locations
To remove the selected program from both your device and this computer, click Remove.
Remove...
OK
Cancel
Help

1. Connect the PDA to the PD on which ActiveSync and the *PDA Client* software is installed.

2. Use Windows' *Add or Remove Programs* feature to remove the *PDA Client* software.

3. When removing the *PDA Client* software from the PC this way, ActiveSync will give you the option of removing the *PDA Client* software from the PDA as well (provided the PDA is connected).

   Click the *Remove...* button to remove the *PDA Client* software from the PDA as well.

Removing the Matrix Monitor Application

Prerequisites: Before removing the *Matrix Monitor* application, make sure the application is not running. If the *Matrix Monitor* application is running, shut it down by right-clicking the *Matrix Monitor* icon in Windows' notification area (also known as the system tray; typically located in the bottom right corner of your screen), then selecting *Exit*. Note that before the application closes, you will be prompted to specify the password required for communicating with your Matrix Monitor.

1. In Windows' *Start* menu, select *Control Panel*, and select *Add or Remove Programs*.

2. In the *Add or Remove Programs* window's list of currently installed programs, select *Milestone XProtect Matrix Monitor*.

3. Click the *Remove* button, and follow the removal instructions.

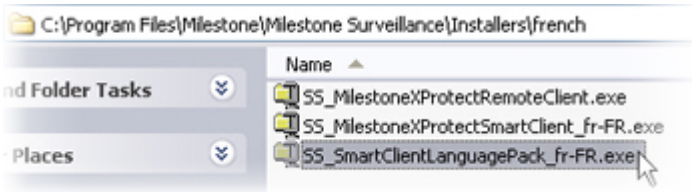
Removing Installation Files for End-User Features

Upon installation of XProtect Enterprise, your surveillance system server by default contains installation files for a number of end-user features. The installation files lets you install the end-user features on the surveillance system server, and make them available to your organization's users through the Download Manager (see page 152).

You can remove installation files for non-required features from the surveillance system server. This can help you save disk space on the server if you know that your organization is not going to use certain features, for example non-relevant language versions:

1. Open the *Installers* folder located in the XProtect Enterprise installation folder, typically at C:\Program Files\Milestone\Milestone Surveillance\Installers.

2. Select the required language sub-folder, then delete the unwanted installation (.exe) files. In the following example, we are about to delete a French *Smart Client* language pack installation file from the surveillance system server:



Glossary

A

Administrator: 1) System administrator. 2) The main application used by surveillance system administrators for configuring the surveillance system server, upon installation or whenever configuration adjustments are required, e.g. when adding new cameras or users to the system.

API: Application Program Interface; a set of tools and building blocks for creating or customizing software applications.

Aspect Ratio: Height/width relationship of an image.

ATM: Abbreviation for Automatic Teller Machine, i.e. a cash dispenser.

AVI: A popular file format for video. Files in this format carry the .avi file extension.

B

Browser: 1) A software application for finding and displaying web pages. 2) In XProtect Enterprise specifically, the term *Browser* may occasionally be used when referring to the *Viewer* application, as the *Viewer* was formerly known under the name *Browser*.

C

Carousel: Feature for displaying video from several cameras, one after the other, in a single camera slot. The required cameras as well as the intervals between changes are specified by the surveillance system administrator. If configured, the carousel feature is available in the *Smart Client*.

Central: Milestone XProtect Central, a product available as an add-on to XProtect Enterprise. XProtect Central provides a complete overview of status and alarms from any number of surveillance system servers, regardless of location.

Codec: A technology for compressing and decompressing audio and video data, for example in an exported AVI file. MPEG and Indeo are examples of frequently used codecs.

D

DirectX: A Windows extension providing advanced multimedia capabilities.

DLK: Device License Key; a registration code required for every device (IP network camera or IP video encoder) installed on the surveillance system. If you do not have system administration responsibilities, you do not have to deal with DLKs. System administrators obtain DLKs as part of the software registration process. System administrators use the Import DLKs... feature in the *Administrator* application to import DLKs into the surveillance system.

DNS: Domain Name System; a system that allows translation between alphabetic host names (example: mycomputer) or domain names (example: www.mydomain.com) and numeric IP addresses (example: 192.168.212.2). Many people find alphabetic names easier to remember than numeric IP addresses.

Driver: A small program used for controlling/communicating with a device.

DST: Daylight Saving Time (a.k.a. summer time), the practice of advancing clocks in order for evenings to have more daylight and mornings to have less.

DVR: Digital Video Recorder.

F

Fisheye: A technology that allows creation and viewing of 360-degree panoramic images.

FPS: Frames Per Second, a measure indicating the amount of information contained in motion video. Each frame represents a still image, but when frames are displayed in succession the illusion of motion is created. The higher the FPS, the smoother the motion will appear. Note, however, that a high FPS may also lead to a large file size when video is saved.

Frame Rate: A measure indicating the amount of information contained in motion video. Frame rate is typically measured in FPS (Frames Per second). The higher frame rate, the smoother motion in video sequence will appear.

FTP: File Transfer Protocol, a standard for exchanging files across the internet. FTP uses the TCP/IP standards for data transfer, and is often used for uploading or downloading files to and from servers.

G

GSM: Global System for Mobile communications, a system for mobile telephony.

GUID: Globally Unique IDentifier; a unique 128-bit number used to identify components on a Windows system.

H

Host: A computer connected to a TCP/IP network. A host has its own IP address, but may - depending on network configuration - furthermore have a name (hostname) in order to make it easily identifiable.

Hotspot: A particular position for viewing enlarged and/or high quality camera video in the Smart Client.

HTTP: HyperText Transfer Protocol, a standard for exchanging files across the internet. HTTP is the standard used for formatting and transmission of data on the world wide web.

I

I/O: Short for Input/Output.

Image Server: The *Image Server* handles access to the surveillance system for remote users logging in with *Remote Clients* or *Smart Clients* (if the *PDA Server* is installed, also *PDA Clients*). The *Image Server* itself does not require separate hardware; it runs as a service on the surveillance system server. Surveillance system administrators handle *Image Server* configuration, including remote users' access rights, through the *Image Server Administrator* application.

IP: Internet Protocol; a protocol (i.e. standard) specifying the format and addressing scheme used for sending data packets across networks. IP is often combined with another protocol, TCP (Transmission Control Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

IP Address: Internet Protocol address; the identifier for a computer or device on a network. Used by the TCP/IP protocol for routing data traffic to the intended destination. An IP address consists of four numbers, each between 0 and 256, separated by full stops (example: 192.168.212.2).

IPIX: A technology that allows creation and viewing of 360-degree panoramic images.

K

Keyframe: Used in the MPEG standard for digital video compression, a keyframe is a single frame stored at specified intervals. The keyframe records the entire view of the camera, whereas the

following frames record only the pixels that change. This helps greatly reduce the size of MPEG files.

M

MAC Address: Media Access Control address, a 12-character hexadecimal number uniquely identifying each device on a network.

Matrix: Feature integrated into XProtect Enterprise, enabling control of live camera views on remote computers for distributed viewing. Once configured, Matrix-triggered live video can be viewed in *Smart Client*s or on computers with the *Matrix Monitor* application installed.

Matrix Monitor: Client application for watching video triggered by the Matrix feature.

Matrix Recipient: Computer on which Matrix-triggered video can be viewed, i.e. a computer with a *Smart Client* or the *Matrix Monitor* application installed.

Monitor: An application used in previous versions of XProtect Enterprise for recording and displaying video. The *Monitor* application has from XProtect Enterprise version 6.5 been superseded by the *Milestone Recording Server Service*.

MPEG: A group of compression standards and file formats for digital video developed by the Moving Pictures Experts Group (MPEG). MPEG standards use so-called lossy compression as they store only the changes between frames, removing often considerable amounts of redundant information: Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reduce the size of MPEG files.

N

NTLM: Abbreviation of Windows NT LAN Manager; a network authentification protocol.

P

Patrolling: The movement of a PTZ camera between two or more preset positions.

PDA: Personal Digital Assistant; a handheld computer device with networking features.

PDA Client: Client application for remote viewing of surveillance video on a PDA.

PDA Server: Image Server front-end required when providing remote access to users logging in with a PDA Client.

PIN: Personal Identity Number (or Personal Identification Number), a number used to identify and authenticate users.

Polling: Regularly checking the state of something, for example whether input has been received on a particular input port of a device. The defined interval between such state checks is often called a polling frequency.

PTZ: Pan/Tilt/Zoom; a highly movable and flexible type of camera.

PUK: Personal Unblocking Key, or PIN Unlock Key, a number used as an extra security measure for SIM cards.

R

Recording: In IP video surveillance systems, the term *recording* means *saving video and, if applicable, audio from a camera in the camera's database on the surveillance system*. In many IP surveillance systems, all of the video/audio received from cameras is not necessarily saved. Saving of video and audio in a camera's database is in many cases started only when there is a reason to do so, for example when motion is detected, when an event occurs, or when a specific period of

time begins. Recording is then stopped after a specified amount of time, when motion is no longer detected, when an event occurs, when a time period ends, or similar. The term *recording* originates from the analog world, where video/audio was not taped until the record button was pressed.

Recording Server Service: A vital part of XProtect Enterprise; recordings are only transferred to the surveillance system while the Recording Server service is running.

Remote Client: Client application for letting remote users access the surveillance system in order to view live video, play back recorded video, activate outputs, print and export evidence, etc. (access to features depend on individual user rights). Users access the *Remote Client* straight from the surveillance system server through an Internet Explorer browser.

S

SDK: Software Development Kit; a programming package enabling software developers to create applications for use with a specific platform.

SIM: Subscriber Identity Module, a small card inserted into a GSM mobile phone, a GSM modem, etc. The SIM card is used to identify and authenticate the user.

SLC: Software License Code; a product registration code required for using the surveillance system software. If you do not have system administration responsibilities, you do not have to deal with SLCs. System administrators use SLCs when installing and registering the software.

Smart Client: Advanced client application for letting remote users access the surveillance system in order to view live video, play back recorded video, activate outputs, print and export evidence, etc. (access to features depend on individual user rights). The *Smart Client* offers considerably more features than its sister application, the *Remote Client*. Such extra features include live and playback audio, digital zoom, timeline browsing, etc. The *Smart Client* should always be downloaded from the surveillance system server and installed locally on remote users' PCs.

SMS: Short Message Service, a system for sending text messages to mobile phones.

SMTP: Simple Mail Transfer Protocol, a standard for sending e-mail messages between mail servers.

Subnet: A part of a network. Dividing a network into subnets can be advantageous for management and security reasons, and may in some cases also help improve performance. On TCP/IP-based networks, a subnet is basically a part of a network on which all devices share the same prefix in their IP addresses, for example 123.123.123.xxx, where 123.123.123 is the shared prefix. Network administrators use so-called subnet masks to divide networks into subnets.

T

TCP: Transmission Control Protocol; a protocol (i.e. standard) used for sending data packets across networks. IP is often combined with another protocol, IP (Internet Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

TCP/IP: Transmission Control Protocol/Internet Protocol; a combination of protocols (i.e. standards) used when connecting computers and other devices on networks, including the internet.

Telnet: A terminal emulation program used on TCP/IP networks. With Telnet, you can connect to a server from a computer on the network, and execute commands through Telnet as if you were entering them directly on the server. Windows includes a client for use with Telnet.

Transact: Product available as an add-on to this surveillance system. Transact handles loss prevention through video evidence combined with time-linked Point-of-Sale or ATM transaction data.

U

UDP: User Datagram Protocol; a connectionless protocol for sending data packets across networks. Primarily used for broadcasting messages. UDP is a fairly simple protocol, with less error recovery features than e.g. the TCP protocol.

URL: Uniform Resource Locator; an address of a resource on the world wide web. The first part of a URL specifies which protocol (i.e. data communication standard) to use when accessing the resource, whereas the second part of the URL specifies the domain or IP address at which the resource is located. Example: http://www.milestonesys.com.

V

Video Encoder: Also known as Video Server. A device, typically a standalone device, which is able to stream video from a number of connected client cameras. Video encoders contain image digitizers, making it possible to connect analog cameras to a network.

Video Server: Other name for Video Encoder.

VMD: Video Motion Detection.

Index

—.—
.Net 174
.Net, Framework Required for PDA Server 180
—3—
3 GB Switching 165
—A—
About Adm, Feature in Administrator Application 30
Absolute Positioning, PTZ 56
Access Client Solution, Choosing a 173
Access Clients 172
Access Clients, Maximum Number of Simultaneously Connected 140
Active Directory 145
Active Directory, How to Import Users from 146
Add New Event Window (for Adding Event Buttons) 98
Add New Event Window (for Devices Handling One Input Only) 88
Add New Event Window (for Devices Handling Several Inputs) 91
Add New Event Window (for Specifying Generic Events) 101
Add New Output Window 94
Adjust Motion Detection Window 50
Administrator Application, About 30
Administrator Log 157
Administrator Login Window 30
Administrator Password 30, 76, 79
Administrator Window 30
Administrator's Getting Started Checklist 21
Advanced Window 95
Alert Port 95
Alerts 72, 78, 80, 82, 89, 92, 98, 99, 104, 130, 131
AND, Boolean Operator 103
Archive Setup Window 130
Archives, Backing Up 128
Archives, Viewing 129
Archiving **125**, 130
Archiving, Dynamic 131, **134**
Archiving, Static 131, **133**
Audio Settings 45, **66**
Audio Source, Disabling/Enabling an 31, 67
Audio Source, Editing Settings of an 31, 67
Audio, Archiving 126, 134

Audio, Important Information about Using 66
Audio, Rights to Use in Access Clients 150
Audit Log 143, 158
—B—
Backing Up Archives 128
Basic Users 145, 146
Browse Tab, Client 149
Buffer, Pre/Post 45
—C—
Calendar, Scheduler's 73
Camera Administration, In Administrator 43
Camera Name and Number Window 64
Camera Settings for [Device Name] [Camera Name] Window 43
Camera Settings for [Device Name] Window 40
Camera Shortcut Numbers, Assigning 31, 41, 64
Camera, Disabling/Enabling a 31
Camera/Alert Scheduler Window 71
Cameras, Adding and Configuring in Administrator 43
Cameras, Renaming 31
Cameras, Start on Remote Live Request 78
Central, XProtect 76, 79
Checklist, Administrator's Getting Started 21
Client Solution, Choosing a 173
Clients 172
Clients, Maximum Number of Simultaneously Connected 140
Configure Device Window 50
Connect (Matrix Configuration Action) 137
Connect then Disconnect (Matrix Configuration Action) 137
Copying/Pasting Schedules 74
Copyright 3
Corrupted Database, Avoiding 163
Corrupted Database, Repairing 48
CPU, Minimum Requirements 16
—D—
Database 44, **46**, 71, 125, 126
Database Repair 48
Database Resizing 48, 128
Database, How Use of Audio Affects 66
Database, Maximum Size 46
Database, Protecting from Corruption 163
Date & Time in Image 50
Daylight Saving Time 168

Define Exclusion Regions Window 52
Define Local IP Ranges Window 144
Define User Rights Window 148
Designate as Master Server 142
Device Drivers 160
Device License Keys, How to Import 35
Device License Keys, How to Obtain 21
Device Manager 30
Device Packs 160
Device Password 37, 40
Device Serial Number ..... *See* MAC Address
Devices, Detection of Motion, Objects, etc. on 90
Digital Video Recorder 36, **42**
DirectX 16
Disabling a Camera 31
Disabling an Audio Source 31
Disclaimer 3
Disconnect (Matrix Configuration Action) 138
Disk Space, Automatic Response if Running Out of 127
DLKs, How to Import 35
DLKs, How to Obtain 21
Domain Controller 145
Download Manager 152
Download Manager, Tree Structure in 153
Download Page 152
Drivers 160
DST 168
DVR 36, **42**
Dynamic Archiving 131, **134**

—E—

Earlier Version, Upgrading from 25
Edit Device Settings Window 38
Edit Event Window (for Editing Event Buttons) 99
Edit Output Window 94
E-Mail Alerts 78, **80**, **82**, 89, 92, 98, 99, 130
E-Mail Alerts, Scheduling 72
E-Mail Setup Window 80
Enable Outside Access, Image Server Option 139
Enabling a Camera 31
Enabling an Audio Source 31
Event Buttons 84, **96**

Event Buttons Window 96
Event Buttons, How to Add 108
Event Indication 54
Event Log 157
Event Message Include, Generic Events 102
Event Priority, Generic Events 102
Event Protocol, Generic Events 101
Event Rule Type, Generic Events 101
Event Substring, Generic Events 102
Event Window (for PTZ Preset Positions on Event) 59
Event, Notification on 54
Event, PTZ Preset Position on 59
Event, Recording on 45
Events 84
Events, Associating with Output 105
Events, Generic 84, **100**
Events, Input 84, 86, 88
Events, Manually Triggered 84, **96**
Events, Recording Video from Before 45
Events, Sending Video to Matrix Recipients on 137
Events, VMD 84, 86
Events. Input 90, 91
Exclamation Mark, Red 137
Exclude Regions, Motion Detection Settings 52
Export Log 158

—F—

F1 Key 28
Falling Signal 89, 92
Firewall 37, 139
Fisheye **46**, **62**
Fisheye Camera Configuration Window 62
Frame Rate, Recording 44
Frame Rate, Speedup 44
FTP Server Port 95

—G—

General Settings Window 76
Generic Events 84, **100**
Generic Events Window 100
Generic Events, How to Add 112
Generic Events, How to Test 114
Getting Started 21

Global Event Buttons 97
Glossary 190
Graphics Adapter, Minimum Requirements 16
GSM Modem 82
—H—
Hard Disk, Minimum Requirements 16
Help System, Built-in **28**, 69
High, Sensor Going 89, 92
—I—
I/O 84
I/O Control Window 105
I/O Devices 85, 96
I/O Setup Window 86
IIS 16
IIS, PDA Server 180, 182
Image Import Service Log 158
Image Quality 50
Image Server 139
Image Server Administrator Window 139
Image Server Log 143, 158
Importing Device License Keys 35
In Sequence Timespan 143
Input 84
Input Events 84, 86, 88, 90, 91
Input Events, How to Add 107
Input/Output Devices 85, 96
Installation, Milestone XProtect Enterprise 24
Integrity Check, Log 159
Internet Information Services 16
IP Address **36**, **39**
IP Address, Local 151
IP Address, Local 139, 144
IP Address, Public 139
IPIX ..... *See* Fisheye
—L—
Language Packs 152
Language packs, Server-Side Installation of 154
Language Support and XML Encoding, Image Server 143
Live Settings 45
Live Tab, Client 149
Local IP Address 139, 140, 144, 151
Local IP Ranges, Image Server Option 140, 144

Log Error Messages 159
Log Integrity Check 159
Log, Administrator 157
Log, Audit 143, 158
Log, Event 157
Log, Export 158
Log, Image Import Service 158
Log, Image Server 143, 158
Log, Recording Server Service 157
Logging 69, **77**, **157**
Logging In, Administrator 30
Loudspeakers 150
Loudspeakers, Associating with Camera 45
Low, Sensor Going 89, 92

—M—

MAC Address 21, 39, 125
Manually Started Recording 76
Manually Triggered Events 84, **96**
Manually Triggered Events, How to Add 108
Manually Triggered Output 106
Manually Triggered Output, How to Add 118
Master Server, Designating a Server as 142
Master/Slave Setup 141, 151
Master/Slave Setup, Upgrading Servers in 142
Matrix 33, 135, 171
Matrix Configuration Window 135
Matrix Monitor Application 171
Max. Number of Clients, Image Server Option 140
Microphone Settings Window 67
Microphone, Associating with Camera 45
Microphones 150
Microphones, Important Information about Using 66
Microsoft Windows Vista, Important Information for Users of 24
Milestone Offices 206
Milestone XProtect Central Settings Window 79
Monitor Application (Discontinued), Alternatives to 170
Motion Detection 45, 46, **50**
Motion Detection, Disabling in Parts of Image 52
Motion Detection, How PTZ Patrolling Should React on 62
Motion Detection, Output on 54, 106
Motion Sensitivity 51

Motion, Recording on 45
Motion, Recording Video from Before 45
Motion-Triggered Output, How to Add 121
Multiple Input Events Window 90
—N—
NAT 37
Network, Minimum Requirements 16
New Timer Window 93
Noise Sensitivity 51
NTLM 145
—O—
Object Detection 90
On Event, Recording 45
On Motion, Recording 45
Online Periods 71
Operating System Virtual Memory 165
Operating System, Minimum Requirements 16
OR, Boolean Operator 103
Output **53**, 84, 86, 94, 105, 106
Output Buttons 54, 106
Output Buttons, How to Add 118
Output Settings for [Device Name] [Camera Name] Window 53, 106
Output, Associating with Events 105
Output, How to Add Manually Triggered 118
Output, How to Add Motion-Triggered 121
Output, Manually Triggered 54, 118
Output, Motion-Triggered 54, 121
Outside Access, Image Server 139
—P—
Pan/Tilt/Zoom 40, **56**, **60**
Pan/Tilt/Zoom, Absolute and Relative Positioning 56
Password 30, 37, 40, 76, 79
Patrol Scheme 60
Patrolling 60
Patrolling on Motion Detection 62
Patrolling, Resuming after Interruption 77
Patrolling, Scheduling 72, 74
Pausing the Recording Server Service 70
PDA Client 173, 179
PDA Server 173, **180**
Polling Frequency 96
Port Numbers 19, 136, 139, 140

Positioning, Absolute and Relative PTZ 56
Pre/Post Buffer 45
Pre-6.0 Version Slaves 142
Preset Positions 56, 59
Preset Positions from Device, Using 58
Preset Positions, Patrolling between 60
Preview Image 50
Previous Version, Upgrading from 25
Private Groups, Client 149
PTZ 40, **56**, **60**
PTZ Patrolling 60
PTZ Patrolling, Resuming after Interruption 77
PTZ Patrolling, Scheduling 72, 74
PTZ Preset Positions 56, 59
PTZ Preset Positions for [Device Name] [Camera Name] Window 56
PTZ Preset Positions from Device, Using 58
PTZ Scanning 62
PTZ, Absolute and Relative Positioning 56
Public IP Address 139

—Q—

Quiet Installation, Smart Client 177

—R—

RAM, Minimum Requirements 16
Recording **44**, 71
Recording Frame Rate 44
Recording on Event 45
Recording on Motion 45
Recording Server Manager 68
Recording Server Service 68
Recording Server Service Log 157
Recording Server Service, Pausing/Resuming 70
Recording Server Service, Starting/Stopping 68
Recording Video from Before Event/Motion Occured 45
Recording, Definition 192
Recording, How Use of Audio Affects 66
Recording, Manually Started 76
Redundancy 141
Registration of Software 21
Relative Positioning, PTZ 56
Remote Access Solution, Choosing a 173
Remote Client 178

Remote Client, Private Groups 149
Remote Client, Server-Side Installation of 154
Remote Client, Shared Groups 149
Remote Live Request, Start Cameras on 78
Removal 186
Renaming Cameras 31
Repair, Database 48
Resuming the Recording Server Service 70
Rising Signal 89, 92
Root Password 37, 40
Router 37, 139
Running Out of Disk Space, Automatic Response if 127

—S—

Scanning, PTZ 62
Scheduling **71**, 78
Sensitivity, Motion 51
Sensitivity, Noise 51
Server-Side Installation of End-User Features 154
Service Manager Window 70
Setup Notifications on Events Window 54
Setup PTZ Patrolling Window 60
Setup Tab, Client 149
Shared Groups, Client 149
Shortcut Numbers, Assigning to Cameras' 31, 41, 64
Signal, Rising/Falling 89, 92
Silent Installation, Smart Client 177
Slave Administration Window 151
Slave Servers 141, 151
Slave Servers, Pre-6.0 Version 142
Slave/Master 141, 151
SLC 30, 141
Smart Client 175
Smart Client, Private Groups 149
Smart Client, Server-Side Installation of 154
Smart Client, Shared Groups 149
Smart Client, Silent Installation of 177
SMS Alerts 78, 89, 92, 99, 104, 131
SMS Alerts, Scheduling 72
SMS Settings Window 82
SMTP 80, 81
SMTP Port 95

Software License Code 30, 141
Software Registration 21
Software Updates 15
Software, Minimum Requirements 16
Speaker Settings Window 67
Speakers 150
Speakers, Associating with Camera 45
Speakers, Important Information about Using 66
Speedup 44
Speedup Frame Rate 44
SSL, E-Mail Alerts Not Working with 81
Standard Time/Daylight Saving Time 168
Start Cameras on Remote Live Request 78
Start Event 72
Starting the Recording Server Service 68
Static Archiving 131, **133**
Status Monitoring 68
Stop Event 73
Stopping the Recording Server Service 68, 70
Subnets 140, 144
Summer/Winter Time 168
Support, Finding License Information if Requiring 30
Support, Finding Version Information if Requiring 30, 70
System Requirements 16
System Status, Monitoring 68

—T—

Target Audience 2
TCP 100, 101
Telnet 114
Text Message, Mobile Phone ..... *See* SMS
Time Server 50
Timer Events 86, **93**, 97
Timer Events, How to Add 116
Timestamp in Image 50
Trademarks 3
Transact 33
Tree Structure in Download Manager 153

—U—

UDP 84, 100, 101
Uninstallation 186
Updates 15

Upgrading from a Previous Version 25
UPS 163
User Administration Window 144
User Administration, in Image Server Administrator window 141
User Rights, Defining for Remote Access 141, **148**
Users, Defining for Remote Access 141, **144**

—V—

Version Information 30, 70
Video Device Drivers 160
Video Encoder 36, 40, 126
Video Encoder, Device License Keys for 21, 35
Video Encoder, PTZ Cameras Attacted to 40
Video Server ..... *See* Video Encoder
Viewer 129, **169**
Viewer, Repairing Archived Corrupted Database with 48
Virtual Memory, Operating System 165
Virus Scanning, Negative Effect on System Performance 162
Vista, Important Information for Users of 24
VMD 45, 46, **50**
VMD Events 84, 86
VMD Events, How to Add 110
VMD, Disabling in Parts of Image 52
VMD, How PTZ Patrolling Should React on 62
VMD, Output on 54, 106

—W—

Welcome Page with End-User Features 152
Windows Users 145, 146
Windows Vista, Important Information for Users of 24
Winter/Summer Time 168

—X—

XProtect Central 79
XProtect Central 76
XProtect Matrix 33, 135, 171
XProtect Transact 33

Milestone Systems offices are located across the world. For details about office addresses, phone and fax numbers, visit www.milestonesys.com.